NETASQ FIREWALL MULTIFONCTIONS

MANUEL D’UTILISATION ET DE CONFIGURATION

Date	Révision	Auteur	Objet
Novembre 2011	V1.0	NETASQ	Création

Référence : nafrgde_FirewallUserGuide.doc

BIENVENUE

Bonjour et bienvenue sur la page d'accueil de l'aide en ligne NETASQ V9.

Vous pouvez naviguer au sein de l'aide en ligne via la colonne de gauche, ou cliquez sur le bouton d'aide en haut à droite de votre interface graphique.

Pour toute question ou si vous souhaitez nous signaler une erreur, contactez-nous sur documentation@netasq.com

ADMINISTRATEURS

Ce module est composé de deux onglets :
- `Administrateurs` : il permet de créer des administrateurs en octroyant des droits d'administration aux utilisateurs utilisant une des méthodes d'authentification suivantes : LDAP RADIUS, KERBEROS, ou SSL.
- `Compte admin` : Cet onglet permet de définir le mot de passe d'authentification du compte admin en exportant la clef publique ou privée.

Onglet « Administrateurs »

L'écran de cet onglet est divisé en trois parties :
- Une barre des tâches (en haut) : celle-ci affiche les différentes actions possibles sur un administrateur (**Ajouter un administrateur**, **Supprimer**, **Copier les droits** etc.).
- La liste des utilisateurs et groupes d'utilisateurs répertoriés en tant qu'admin (à gauche).
- La grille des droits des administrateurs (à droite).

Les manipulations possibles

Vous allez pouvoir constituer votre grille d'administrateurs issus de votre base LDAP ainsi que leurs droits respectifs

Ajouter un administrateur

Ajouter un administrateur sans droit	Ce type d'administrateur dispose des droits de base à savoir l''accès au **Dashboard** et aux modules suivants : **Licence, Maintenance, Active Update,** la **Haute disponibilité** et son assistant, la console **CLI, Réseau, Routage, DNS dynamique, DHCP, Proxy cache DNS**, les Objets, les groupes d'URL, **Certificats et PKI,** l'**Authentification** et son assistant, le **Filtrage URL, SSL** et **SMTP, Alarmes, Profils d'inspection, Antivirus, Antispam, Détection de vulnérabilités, Messages de blocage,** et les Préférences.
Ajouter un administrateur avec accès en lecture seule	Ce type d'administrateur dispose des mêmes accès de base que l'admin « sans droits » avec en plus des droits supplémentaires : la lecture des logs **SNMP, Alertes e-mails, Evénements système,** ainsi que la lecture du **Filtrage** et du **VPN.**
Ajouter un administrateur avec tous les droits	Ce type d'administrateur aura accès à tous les modules exceptés Configuration, Administrateurs, et Configuration de l'annuaire (LDAP). **REMARQUE** Il n'existe qu'un seul « super-administrateur » qui présente les caractéristiques suivantes : - Il est le seul à être habilité à se connecter via la console locale sur les boîtiers NETASQ, et ce uniquement lors de l'installation du firewall ou pour des opérations de maintenance, en dehors de l'exploitation. - Il est chargé de la définition des profils des autres administrateurs. - Tous les accès dans les locaux où sont stockés les boîtiers firewalls, ainsi que les interventions effectuées se font sous sa surveillance.

Une fois votre administrateur importé, il apparait dans la liste « **Utilisateur – groupe d'utilisateur** » à gauche de l'écran.
Vous pouvez effectuer diverses actions sur celui-ci.

Supprimer	Sélectionnez l'administrateur à retirer de la liste et cliquez sur **Supprimer**.
Monter	Placer l'administrateur au-dessus du précédent dans la liste.
Descendre	Placer l'administrateur au-dessous du suivant dans la liste.
Copier les droits	Sélectionnez l'administrateur dont vous souhaitez copier les droits et cliquez sur ce bouton.
Coller les droits	Sélectionnez l'administrateur auquel vous souhaitez attribuer les mêmes droits que celui que vous venez de copiez et cliquez sur ce bouton.
Donner tous les droits	Quelques soient les droits attribués à l'administrateur sélectionné, en cliquant sur ce bouton,

La grille des droits

Votre interface est en « **vue simple** » par défaut. La grille affiche 5 colonnes représentant les 5 catégories de droits auquel un administrateur est affilié ou non : **Système, Réseau, Utilisateurs, Firewall** et **Supervision**.

Les icônes de la grille ont la signification suivante :

 : L'ensemble des droits sont attribués.

 : L'ensemble des droits ne sont pas accordés.

 : Une partie des droits sont accordés, d'autres non.

En passant en « **vue avancée** » à l'aide de l'icône ou (en fonction de la longueur de votre écran), la grille affichera le détail des droits par catégorie. Pour connaître précisément les droits correspondant à chaque colonne, une bulle informative est disponible sur l'en-tête de chacune d'entre elles.

Exemple

Si vous vous positionnez en haut de la colonne **Système,** vous verrez apparaître les accès qu'elles incluent, à savoir les droits de « *Maintenance, Objets* ».

 **NOTES**

Un double clic sur les icônes représentées change l'état des permissions (de « accordé » à « non accordé » par exemple).

Un double clic sur cette icône accordera les droits, et celle-ci la remplacera à l'affichage.

Onglet « Compte admin »

Cet écran va permettre de définir les données d'authentification du compte administrateurs.

Mot de passe	Définition du mot de passe du compte admin. **REMARQUE** Il ne doit pas contenir le caractère ".
Confirmer le mot de passe	Confirmation du mot de passe du compte admin, que vous venez de renseigner dans le champ précédent
Force du mot de passe	Ce champ indique le niveau de sécurité de votre mot de passe : « Très Faible », « Faible », « Moyen », « Bon » ou « Excellent ». Il est fortement conseillé d'utiliser les majuscules et les caractères spéciaux.

NOTE

NETASQ utilise un système de chiffrement dit « asymétrique », à savoir qu'il utilise une paire composée d'une clef publique, servant à chiffrer les données, et d'une clef privée, servant à déchiffrer. L'intérêt de cette utilisation est qu'elle supprime le problème de transmission sécurisée de la clé, et permet la signature électronique.

Exporter la clef privée	En cliquant sur ce bouton, vous enregistrerez la clef privée associée au compte admin sur votre machine.
Exporter la clef publique	En cliquant sur ce bouton, vous enregistrerez la clef publique associée au compte admin sur votre machine.

ACTIVE UPDATE

Le module d'`Active Update` se compose d'un seul écran de configuration :

Cet écran se divise en 2 parties :

- **Mises à jour automatiques** : permet l'activation d'un module de mise à jour.
- **Configuration avancée- Serveurs de mise à jour**: permet de définir les serveurs de mise à jour.

Mises à jour automatiques

Activé	Activation (boutons Activé/ Désactivé) ou non (par un simple clic) de la mise à jour via l'Active Update pour le type de mise à jour sélectionné.
Module	Type de mise à jour. (La liste des modules varie selon la licence acquise).



NOTES
Un retour arrière automatique est effectué en cas d'échec de la mise à jour.
Vous pouvez autoriser (bouton **« Tout autoriser »**) ou interdire (bouton « **Tout inderdire** ») toutes les mises à jour en un double-clic.

Serveurs de mise à jour

URL	Les fichiers de mise à jour sont récupérés sur un des serveurs définis par l'utilisateur. (Les serveurs de mise à jour sont communs à tous les types de mise à jour.) 4 URL sont définies par défaut. Pour ajouter une URL, cliquez sur **Ajouter** ; l'url suivante est ajoutée par défaut : http://update.netasq.com/1. Remplacez par votre adresse URL puis cliquez sur **Appliquer**. Pour supprimer une URL de la liste, sélectionnez-là puis cliquez sur **Supprimer**.

Vous pouvez **Ajouter** une URL en cliquant sur l'icône , et sur pour la **Supprimer**

Fréquence de mise à jour	Indication de la fréquence des mises à jour des listes d'URL dynamiques, des signatures contextuelles ASQ et de la configuration de l'antispam. La fréquence est indiquée à 3 heures, la modification de cette fréquence peut se faire via le mode Console.

AGENT SNMP

L'écran de configuration du service `SNMP` se compose de trois onglets :

- **`Général`** : onglet qui s'affiche par défaut lorsque l'on clique sur le menu SNMP dans l'arborescence de gauche et qui permet l'activation du module et les notifications alarmes et système qui seront intégrés dans les MIB (Management Information Base) disponibles (en consultation et en envoi de traps).
- **`SNMPv3` :** Version recommandée car munie d'outils plus sécurisés (outils de sécurité comme l'authentification, le cryptage, le contrôle du timing…).
- **`SNMPv1 – SNMPv2c`** : Version dont la requête SNMP contient un nom appelé « Communauté » utilisé comme identifiant et transmis en clair sur le réseau.

L'onglet « Général »

Cet onglet permet de configurer le système, c'est-à-dire la machine et son administrateur, contient les notifications (alarmes et événements système) qui seront intégrés dans les MIB disponibles.
L'option **Activer l'agent** permet l'activation du module. Il est possible toutefois de configurer les données de cet écran même si le module n'est pas activé.

SNMPv3 (recommandé)	Active la version 3 de snmp, version recommandée car munie d'outils plus sécurisés (outils de sécurité comme l'authentification, le cryptage, le contrôle du timing…). Depuis décembre 2002, un nouveau standard existe pour le protocole SNMP, il apporte une avancée significative en matière de sécurité. La configuration requiert les paramètres suivants : SNMPv3 offre des méthodes d'authentification ainsi que des méthodes de chiffrement, et résout certains problèmes de sécurité des versions précédentes.
SNMPv1/v2c	Active les versions v1/v2C de SNMP. V1 est la première version du protocole. La seule vérification faite par cette version concerne la chaîne de caractères « Community ». La version v2C est une version qui améliore les types d'opération de SNMPv2p et utilise la sécurité par chaîne de caractères « community » de SNMPv1.
SNMPv1/v2c et SNMPv3	Active les trois versions de SNMP.

Configuration des informations MIB-II

Emplacement (sysLocation)	Information alphanumérique de lieu sur l'élément surveillé. La localisation peut indiquer un pays, une ville, une salle serveur, etc. *Exemple : France.*
Contact (sysContact)	Adresse e-mail, n° de téléphone, etc. de la personne à contacter en cas de problème. *Exemple : admin@netasq.com*

Envoi des alertes SNMP (traps)

Alarmes de prévention d'intrusion	**Ne pas envoyer** : en cochant cette option, vous ne recevrez pas les alarmes ASQ. En cochant **Envoyer uniquement les alarmes majeures**, vous pourrez recevoir les alarmes ASQ majeures. En cochant **Envoyer les alarmes majeures et mineures**, les alarmes majeures et mineures ASQ seront émises.
Evénements systèmes	En cochant **ne pas envoyer**, vous ne recevrez pas les alarmes système. En cochant **envoyer uniquement les alarmes majeures**, vous pourrez recevoir les alarmes système majeures. En cochant **envoyer les alarmes majeures et mineures**, les alarmes systèmes majeures et mineures seront émises.

L'onglet « SNMPv3 »

Les options **Activer l'agent SNMPv3 (recommandé)** ou **SNMPv1/v2c et SNMPv3** permettent l'activation du module SNMP v3.

Connexion à l'agent SNMP

Nom d'utilisateur	Nom d'utilisateur utilisé pour la connexion et pour la consultation des MIB sur le firewall.

Authentification

Mot de passe	Mot de passe de l'utilisateur qui consultera les MIB.
Algorithme	Deux types d'authentification sont disponibles, le MD5 (algorithme de hachage qui calcule un condensé de 128 bits) et le SHA1 (algorithme de hachage qui calcule un condensé de 160 bits). Par défaut, l'authentification se fait en MD5.

Chiffrement (optionnel)

Mot de passe	Les paquets SNMP sont chiffrés en DES ou AES (*Advanced Encryption Standard*), une clé de chiffrement peut être définie. Par défaut c'est la clé d'authentification qui est utilisée. **AVERTISSEMENT** Il est vivement recommandé d'utiliser une clé spécifique**.**
Algorithme	Les deux types de chiffrement possibles sont DES et AES. Par défaut le chiffrement se fait en DES.

Envoi des alertes SNMPv3 (traps)

L'envoi des traps vers des machines se compose de deux parties avec, à gauche, la liste des machines et à droite le détail d'une machine préalablement sélectionnée.

Liste des serveurs SNMP

Dans cet écran, vous configurez les stations que doit contacter le firewall lorsqu'il veut envoyer un Trap SNMP (événement). Si aucune station (machine) n'est spécifiée, le firewall n'envoie pas de messages.
Un assistant vous guide dans la configuration des machines.
En cliquant à droite d'un nom de machine, la base d'objets s'affiche vous permettant de sélectionner une machine.

Serveur [Nom du serveur de destination (objet)]

Les paramètres de la configuration des événements de type SNMP V3 sont les suivants :

Port	Port utilisé pour envoyer les données à la machine (snmptrap par défaut).
Nom d'utilisateur (securityName)	Nom de l'utilisateur autorisé à envoyer un trap sur la station de gestion.
Identifiant (engineID)	Chaîne en hexadécimal créée par la station de gestion pour identifier l'utilisateur de manière unique de type 0x0011223344. Le moteur ID doit être composé au minimum de 5 octets et au maximum de 32 octets.
Niveau de sécurité	Différents niveaux de sécurité sont disponibles pour la version du protocole SNMP : • **Aucun** : aucune sécurité. Les parties « Security Level : authentification » et « Security level : Chiffrement » sont grisés. • **Authentification, pas de chiffrement** : authentification sans chiffrement des traps. • **Authentification et chiffrement** : si le mot de passe chiffrement reste vide on utilise le mot de passe authentification pour le chiffrement.

Paramètres d'authentification

Mot de passe	Mot de passe de l'utilisateur.
Algorithme	Deux types d'authentification sont disponibles, le MD5 (algorithme de hachage qui calcule un condensé de 128 bits) et le SHA1 (algorithme de hachage qui calcule un condensé de 160 bits). Par défaut, l'authentification se fait en MD5.

Paramètres de chiffrement

Mot de passe	Les paquets SNMP sont chiffrés en DES ou AES, une clé de chiffrement peut être définie. Par défaut c'est la clé d'authentification qui est utilisée. **AVERTISSEMENT** **Il est vivement recommandé d'utiliser une clef spécifique.**
Algorithme	Les deux types de chiffrement possibles sont DES et AES. Par défaut le chiffrement se fait en AES.

L'onglet « SNMPv1 - SNMPv2c »

L'option **Activer SNMPv1/v2c** ou **SNMPv1/v2c et SNMPv3** permet l'activation du module SNMP V1 et V2c.

Connexion à l'agent SNMP

Communauté	Les premières versions du protocole **SNMP** ne sont pas sécurisées. Le seul champ nécessaire est le nom de la communauté. Par défaut le RPV (*Réseau Privé Virtuel*) propose le nom "public". **AVERTISSEMENT** Nous vous conseillons toutefois de ne pas l'utiliser pour des raisons de sécurité. Si vous souhaitez indiquer plusieurs communautés, séparez-les par des virgules.

Envoi des alertes SNMPv2c (traps)

Liste des serveurs SNMP

Serveur de destination (objet)	Machine recevant les traps, (objet de type « Machine »).
Port	Port utilisé pour envoyer les traps à cette machine (objet de type : service). Par défaut, snmp trap.
Communauté	Indication de la communauté.

Envoi des alertes SNMPv1 (traps)

Par défaut, la liste des machines recevant de traps V1 est minimisée pour orienter l'utilisateur vers la version V2c.

Liste des serveurs SNMP

Machine	Machine recevant les traps, (objet de type « Machine »).
Port	Port utilisé pour envoyer les TRAPS à cette machine (objet de type : service). Par défaut snmp trap.
Communauté	Indication de la communauté.

ALARMES

Ce module va vous permettre de gérer la configuration de vos alarmes.
Il est découpé en deux vues :

- « vue par profil d'inspection » (aussi appelé « vue par configuration »)
- « vue par contexte » (aussi appelé « vue par protocole »)

Vue par profil d'inspection

Cet écran représente la vue par configuration ou par profil d'inspection des alarmes présentes.



NOTE
Une configuration est un ensemble de profils protocolaires. L'association est définie dans le module « Profils d'inspection ».
Il est possible de trier les alarmes, de les filtrer par une présélection (DoS, IM, etc...) ou de les filtrer grâce à un mot clef. Le résultat est paginé.

Sélection du profil de configuration

Vous pouvez configurer jusqu'à 10 profils, portant par défaut les noms de « Config », « Config 1 » etc. Ces noms ne sont pas modifiables dans le module `Alarmes` mais au sein du menu `Protection applicative\Profils d'inspection` :

1. Sélectionnez une configuration au sein de la liste déroulante.
2. Cliquez sur le bouton « Editer » et sélectionnez « Renommer ».
3. Changez ensuite le nom du profil dans l'emplacement prévu à cet effet et ajoutez un commentaire si besoin.
4. Cliquez sur « Mettre à jour ».

Vous retrouvez votre profil modifié dans la liste déroulante des configurations du module `Alarmes`.

Au sein d'un profil, vous pouvez effectuer plusieurs actions :

Appliquer un modèle

Internet	En appliquant ce modèle, la plupart des niveaux d'alarmes passeront en « Ignorer ».
Basse	En appliquant ce modèle, la plupart des niveaux d'alarmes passeront en « Mineur ».
Moyenne	En appliquant ce modèle, les niveaux d'alarmes seront modifiés en fonction du profil choisi.
Haute	En appliquant ce modèle, la plupart des niveaux d'alarmes passeront en « Majeur ».

Nouvelles alarmes

Tout approuver	En sélectionnant cette option, toutes les nouvelles alarmes matérialisées par l'icône seront acceptées : l'icône disparaîtra et la colonne action concernant ses alarmes affichera « Autoriser ».

Rechercher

Cet emplacement permet de n'afficher que la ou les alarmes contenant la lettre ou le mot saisi.

Présélection

Cette liste contient les différents protocoles et services pris en charge par les alarmes, vous pouvez effectuer un tri et n'afficher que les alarmes faisant partie des catégories suivantes :

Aucune	Toutes les alarmes seront affichées, sans distinction de catégorie.
Nouvelles alarmes	Seules les nouvelles alarmes, matérialisées par l'icône seront affichées (en règle générale, de type id ftp ou http).
VoIP	Seules les alarmes relatives à la Voix sur IP seront affichées (protocoles mgcp, rtcp ou SIP).
Déni de service	Seules les alarmes relatives aux attaques par déni de service (DoS) seront affichées.
Messagerie instantanée	Seules les alarmes relevant une anomalie au niveau des services de messagerie instantanée (MSN, Yahoo Messenger etc.) apparaîtront à l'écran.
Peer to peer	Seules les alarmes relatives aux systèmes peer-to-peer seront affichées.

Les différentes colonnes

Contexte : id	Intitulé de l'alarme.
Message	Texte décrivant l'alarme et ses caractéristiques.
Action	Lorsqu'une alarme est remontée, le paquet qui a provoqué cette alarme subit l'action associée. Vous pouvez choisir d'**Autoriser ou** d'**Interdire** un trafic qui remonte une alarme.
Niveau	Trois niveaux d'alarmes sont disponibles, "Ignorer", "Mineur" et "Majeur".
Nouveau	Permet de visualiser les nouvelles alarmes, matérialisées par l'icône .
Avancé	Cette colonne affiche le choix de la réaction lorsque l'alarme est déclenchée (en plus de l'action **Autoriser** ou **Interdire**). Une fenêtre apparaît et vous propose : **Aucun** : aucune action ne sera effectuée pour cette alarme. **Envoyer un e-mail** : un e-mail sera envoyé au déclenchement de l'alarme. **Mettre en quarantaine** : le paquet responsable de l'alarme sera bloqué. Vous pouvez également choisir de capturer le paquet responsable de la remontée de l'alarme en cochant la case correspondante. La capture pourra être visualisée grâce à un analyseur de réseau (sniffer). Cliquez ensuite sur **Appliquer**.

Pour chacun des 10 profils, vous pouvez effectuer la configuration comme vous le souhaitez, en en modifiant les paramètres décrits ci-avant.

Vue par contexte

Cette vue présente les alarmes par profils protocolaires. La première liste déroulante, à gauche, permet de sélectionner le contexte protocolaire.

Pour chaque protocole, vous pouvez paramétrer jusqu'à 10 fichiers de configuration, sélectionnables grâce à la seconde liste déroulante (affichant « default »)
Vous pouvez changer le nom du fichier en vous reportant dans le menu `Protection applicative\Protocoles et applications :`

1. Sélectionnez une configuration au sein de la liste déroulante.
2. Cliquez sur le bouton « Editer » et sélectionnez « Renommer ».
3. Changez ensuite le nom du profil dans l'emplacement prévu à cet effet et ajoutez un commentaire si besoin.
4. Cliquez sur « Mettre à jour ».

Vous retrouvez votre profil modifié dans la liste déroulante des fichiers de configuration du module `Alarmes`.
Au sein d'un profil, vous pouvez effectuer plusieurs actions :

Modifier la politique

Internet	En appliquant cette politique, la plupart des niveaux d'alarmes passeront en « Ignorer ».
Basse	En appliquant cette politique, la plupart des niveaux d'alarmes passeront en « Mineur ».
Moyenne	En appliquant cette politique, les niveaux d'alarmes seront modifiés en fonction du profil choisi.
Haute	En appliquant cette politique, la plupart des niveaux d'alarmes passeront en « Majeur ».

REMARQUE
La politique choisie apparaîtra entre parenthèses à côté du bouton.

Nouvelles alarmes

Tout approuver	En sélectionnant cette option, toutes les nouvelles alarmes matérialisées par l'icône seront acceptées : l'icône disparaîtra.

Rechercher

Cet emplacement permet de n'afficher que la ou les alarmes contenant la lettre ou le mot saisi.



NOTE GENERALE
Vous pouvez à tout moment, selon la vue dans laquelle vous vous trouvez, basculer dans l'autre en cliquant sur les boutons suivants (en haut à droite de l'écran):
Passer en vue par profil d'inspection ou Passer en vue par contexte

A partir de la version 9.0.1, un champ de recherche instantanée apparaît au sein des deux vues du module, afin de filtrer plus facilement les profils et les contextes, sans devoir appuyer sur « Entrée ».

Une nouvelle alarme a été ajoutée pour détecter le trafic Cisco WAN Optimizer. Par défaut, le trafic est bloqué par l'alarme, mais il est possible de l'autoriser (tcpudp : 247).

ATTENTION
Une fois autorisé, ce type de trafic ne bénéficie pas d'analyse protocolaire.

ALERTES E-MAILS

L’écran se décompose en trois parties :

- L’onglet Configuration : permet de procéder aux réglages de base du module comme le paramétrage du serveur SMTP, la fréquence d’envoi des e-mails (en minutes), les alarmes de prévention d’intrusion et les événements système.
- L’onglet Destinataires : permet de définir les groupes qui seront utilisés dans les politiques de mailing mais aussi dans d’autres modules de configuration où l’envoi de mails est nécessaire.
- L’onglet Modèles : visualisation et modification des formats de mails, utilisés lors de l’envoi des notifications aux utilisateurs et aux administrateurs.

L’onglet « Configuration »

Cet onglet regroupe tous les paramètres nécessaires à la configuration des alertes e-mails.
L’écran comporte les éléments suivants :

Activer les notifications par e-mail

Cette option active la configuration des messages d’alertes. En cas de désactivation, aucun élément de configuration ne sera accessible car le firewall n'enverra pas de mail. Cette option à cocher est désactivée par défaut.


REMARQUE
La notification des e-mails nécessite un serveur de messagerie capable de recevoir les e-mails provenant du firewall.

Serveur SMTP

Serveur	Ce champ détermine la machine (serveur SMTP) à laquelle le firewall va envoyer les mails, en la sélectionnant dans la base d'objets. Par défaut, ce champ est vide.
Port	Port du serveur SMTP où seront envoyés les e-mails. Une liste permet de sélectionner un objet, dont la valeur indiquée par défaut est « SMTP ».
Domaine DNS	Utile pour indiquer le nom de domaine de l'émetteur des e-mails. L'adresse e-mail de l'émetteur sera alors indiquée comme suit : <nom_du_firewall>@<nom_de_domaine>.

Fréquence d’envoi des e-mails (en minutes)

Fréquence d’envoi	Cette option vous permet de spécifier la fréquence d'envoi des rapports. Un rapport contient toutes les alarmes détectées depuis le rapport précédent. Ainsi, la réception du mail s'effectue par tranche horaire et non par alarme déclenchée. La valeur indiquée par défaut est 15.

Alarmes de prévention d'intrusion

Ici, vous pouvez notifier un groupe qui recevra les alarmes de prévention d'intrusion.
La liste des alarmes est envoyée dans le corps de l'e-mail au groupe spécifié.
Le délai d'envoi du rapport des alarmes se modifie dans le champ « Fréquence d'envoi » du menu **Fréquence d'envoi des e-mails (en minutes)**.

Exemple

Si vous spécifiez un envoi toutes les 15 minutes dans le champ « Fréquence d'envoi », vous serez averti par e-mail toutes les 15 minutes des alarmes déclenchées durant ce laps de temps sur le firewall.

Ne pas envoyer	Pas d'envoi de rapport des alarmes de prévention d'intrusion. Ce bouton radio est coché par défaut.
Envoyer uniquement les alarmes majeures	En cochant cette option, le groupe que vous sélectionnerez dans le champ suivant recevra les alarmes majeures.
Destinataire du message	Choix du groupe qui recevra les alarmes de prévention d'intrusion majeures.
Envoyer les alarmes majeures et mineures	En cochant cette option, le groupe que vous sélectionnerez dans le champ suivant recevra les alarmes de prévention d'intrusion majeures et mineures.
Destinataire du message	Choix du groupe qui recevra les alarmes de prévention d'intrusion majeures et mineures.

Evénements système

Tout comme le champ précédent, un groupe peut également être notifié pour recevoir les événements système.
Le délai d'envoi des évènements système se modifie, de la même façon, dans le champ « Fréquence d'envoi » du menu **Fréquence d'envoi des e-mails (en minutes)**.

Ne pas envoyer	Pas d'envoi des événements système. Ce bouton radio est coché par défaut.
Envoyer uniquement les alarmes majeures	En cochant cette option, le groupe que vous sélectionnerez dans le champ suivant recevra les évènements système majeurs
Destinataire du message	Choix du groupe qui recevra les évènements système majeurs.
Envoyer les alarmes majeures et mineures	En cochant cette option, le groupe que vous sélectionnerez dans le champ suivant recevra les évènements système majeurs et mineurs.
Destinataire du message	Choix du groupe qui recevra les évènements système majeurs et mineurs.



L'état des événements système est visible dans un module portant le même nom : Dans le menu, vous pouvez vous rendre dans `Notifications\Evénements système`.

L'onglet « Destinataires »

L'écran se compose de 2 vues:

- Groupes de destinataires
- Sélectionnez un groupe

Un groupe contient un certain nombre d'adresses e-mails.
Il est possible de créer jusqu'à 50 groupes.
Il n'existe aucun groupe préconfiguré. Vous pouvez ajouter de nouveaux groupes, et commentaires, ou encore les supprimer.
Un groupe doit contenir au moins une adresse e-mail. Le nombre d'adresses e-mails dans un groupe est indéfini.

Il sera possible ensuite de choisir un groupe pour l'envoi des rapports de vulnérabilités, détaillés ou simplifiés dans le menu `Protection Applicative => Détection de vulnérabilités.`

Créer un groupe

1. Cliquez sur le bouton **Nouveau groupe de destinataires.** Une ligne supplémentaire s'affiche dans la liste et vous demande de saisir le nom que vous souhaitez donner à votre groupe.
2. Vous pouvez attribuer un commentaire à ce groupe, en vous positionnant sur « Commentaire » et en remplissant le champ prévu à cet effet.

Pour ajouter un destinataire, positionnez-vous sur le groupe choisi. Son nom s'affiche sur la droite, dans le champ **Destinataire membre du groupe : <nomdugroupe>**. Cliquez ensuite sur le bouton **Ajouter un destinataire au groupe**. Un écran s'affiche permettant d'indiquer soit le mail du destinataire soit l'utilisateur ou le groupe auquel il appartient si celui-ci se trouve dans la base d'objets. La saisie de l'adresse e-mail est libre mais le format de l'adresse est vérifié.

Supprimer un groupe

1. Sélectionnez la ligne à supprimer.
2. Cliquez sur le bouton Supprimer. Le message suivant « *Voulez-vous vraiment supprimer le groupe nommé <nom du groupe> ?* » s'affiche. En cliquant sur Oui, le groupe est supprimé de la liste.

REMARQUE
La suppression d'un groupe ne peut être réalisée que si le groupe n'est pas utilisé dans une autre configuration du firewall.
Si l'on veut supprimer un groupe déjà actif dans un module, un pop-up d'avertissement s'affiche et propose de : forcer la suppression, de vérifier l'utilisation du groupe, ou d'annuler l'action.

Vérifier

Le bouton **Vérifier l'utilisation** permet de vérifier si un groupe d'e-mails est utilisé dans les différents modules de configuration du firewall.

1. Sélectionnez la ligne à vérifier.
2. Cliquez sur le bouton **Vérifier** afin d'effectuer la vérification.

L'onglet « Modèles »

Il permet d'utiliser un courrier type personnalisable, pour l'émission des mails. Six modèles sont disponibles, contenant chacun, un corps qui diffère selon le message que l'on veut envoyer.

Edition du modèle (HTML)

Chaque modèle comporte du contenu appelé "body" (comme pour une page HTML). Ce contenu est un texte au format libre qui peut contenir des balises HTML simples afin de finaliser la mise en forme. Ces modèles sont modifiables. Ils peuvent contenir des mot-clés qui seront remplaçés ensuite par des valeurs. Par exemple, un mot-clé peut afficher de manière automatique le nom de l'utilisateur. Pour modifier un contenu, il suffit de cliquer sur le bouton **Modifier**.

L'écran se subdivise en 2 parties :

- En haut : l'aperçu du modèle d'e-mail
- En bas : l'écran de modification

2 boutons vous permettent de modifier le corps du message :

Insérer une variable	Ce bouton vous permet de sélectionner des variables qui seront ensuite remplacées par des valeurs réelles lors de l'envoi du message.
Appliquer le modèle par défaut	Permet de réinitialiser le modèle à sa présentation initiale. Lorsque vous cliquez sur ce bouton, le message suivant s'affiche : "*Voulez-vous vraiment réinitialiser le contenu de ce modèle à sa valeur par défaut ?*"

Vulnérabilités détectées

- Vulnérabilités détectées (détaillées) : modèle de rapport de vulnérabilités détaillé, appliqué par défaut.
- Vulnérabilités détectées (résumées) : modèle de rapport de vulnérabilités simple, appliqué par défaut.

Demande de certificat

- Accepter la demande de certificat : modèle de mail spécifiant que la demande de certificat a été approuvée par l'administrateur.
- Refuser la demande de certificat : modèle de mail spécifiant que la demande de certificat a été rejetée par l'administrateur

Enrôlement d'un utilisateur

- Accepter la requête utilisateur : modèle de mail spécifiant que la demande d'enrôlement a été approuvée par l'administrateur.
- Refuser la requête utilisateur : modèle de mail spécifiant que la demande d'enrôlement a été rejetée par l'administrateur.

Liste des variables

Modèles de mails dédiés à la détection de vulnérabilités:

- Sujet du message ($Title)
- Sous-titre ($SubTitle)
- Résumé du message ($MailSummary)
- Résumé des vulnérabilités ($VulnSummary)
- Machines affectées ($HostsByVuln)
- Applications vulnérables ($VulnByProduct)
- Pied de page du message ($Footer)

Modèles de mails utilisés pour la demande de certificat et l'enrôlement de l'utilisateur.

- Nom de l'utilisateur ($LastName)
- Prénom de l'utilisateur ($FirstName)
- Date de la demande d'enrôlement ($Date)
- Identifiant de l'utilisateur ($UID)
- URL de téléchargement du certificat ($URL)

Exemple de rapport reçu par e-mail pour les alarmes

Type	Minor
Action	Block
Date	2010-10-11 15:08:32
Interface	dmz2
Protocol	tcp
Source	10.2.18.5:55987 (ed:ephemeral_fw_tcp)
Destination	66.249.92.104:80 (www.google.com)
Description	Prévention injection SQL : instruction OR suspecte dans l'URL

ANTISPAM

L'écran de configuration de l'antispam se compose de 3 onglets :

- Général : Configuration de base du module Antispam (activation, paramètres SMTP, Analyse par réputation…).
- Domaines en liste blanche : contient la liste des domaines qui doivent être systématiquement considérés comme légitimes.
- Domaines en liste noire : contient la liste des domaines qui doivent être systématiquement considérés comme spammeurs.

L'onglet «Général »

L'activation de l'antispam s'effectue en déterminant quelles seront les analyses activées. Deux choix sont disponibles sur le firewall :

Activer l'analyse par réputation (listes noires DNS –RBL)	Cette option permet de valider l'émetteur auprès d'une liste publique de Spams reconnue (DNSBL).
Activer l'analyse heuristique	Cette option permet d'étudier le contenu du mail pour en déterminer la portée.

Paramètres SMTP

Le serveur de confiance concerne le serveur SMTP. En renseignant ce champ, qui est facultatif, les e-mails seront analysés de manière plus fine par le module **Antispam**.

Nom du serveur SMTP (FQDN)	Le serveur local **SMTP** désigne le nom canonique de votre serveur SMTP. Cette information est facultative, si elle est renseignée, le module **Antispam** analysera plus finement les e-mails relayés par de multiples serveurs.
Action	Il existe 4 actions possibles qui permettent au proxy SMTP de répondre au serveur SMTP distant en indiquant un rejet pour cause de spam. - **Marquer comme spam** : les mails ne sont pas bloqués mais sont marqués comme spams. - **Bloquer tous les spams** : le mail est rejeté quelque soit le seuil de confiance. - **Bloquer les spams de niveau 2 ou supérieur** : cette option permet de définir qu'à partir du seuil de confiance de niveau 2, un mail sera rejeté. Les seuils sont : « 1 – Bas», « 2 – Moyen», « 3 – Haut». - **Bloquer uniquement les spams de niveau 3** : cette option permet de définir qu'à partir du seuil de confiance 3 (Haut), le mail sera rejeté.

Pour exemple : si vous configurez au niveau de l'analyse heuristique un seuil de 500, les mails seront considérés comme spam à partir de 500. De 500 à 2000, le niveau de confiance sera faible, de 2000 à 3500, il sera modéré, de 3500 à 5000, il sera élevé. Si vous avez indiqué au niveau de cette option un seuil de confiance modéré, tous les mails de niveau modéré et élevé (donc de 2000 à 5000) seront rejetés alors que ceux de 500 à 2000 seront gardés.



REMARQUE
Lorsque plusieurs méthodes d'analyses sont utilisées simultanément, le plus haut niveau de score est attribué.

Configuration avancée

Les messages identifiés comme spam ne sont pas supprimés par le module **Antispam** du boîtier UTM NETASQ. Cependant il effectue des actions de modifications du message détecté comme spam de façon à permettre un traitement futur par le client de messagerie Web par exemple. Deux actions de marquage sont disponibles :

Marquage du sujet des spams (préfixe)	Le sujet des messages identifiés comme spam sont préfixés par la chaîne de caractères définie. Par défaut cette chaîne est **(SPAM *)** où ***** représente le niveau de confiance accordé. Ce score peut varier de 1 à 3. Plus ce score est élevé, plus il est probable que le courrier soit du pourriel. Quelle que soit la chaîne de caractères utilisée, il est indispensable de prévoir l'insertion du niveau de confiance dans cette chaîne en utilisant ***.** Cet * sera ensuite remplacé par le score. La longueur maximale du préfixe peut être de 128 caractères. Les courriers identifiés comme spam sont acheminés et non supprimés.  **AVERTISSEMENT** Les caractères guillemets double ne sont pas autorisés.
Insérer les en-têtes X-Spam	En cochant cette option, le module **Antispam** ajoute au message identifié comme spam, un en-tête synthétisant le résultat de son analyse pour ce message. Cet en-tête antispam, au format "spam assassin" peut ensuite être utilisé par le client de messagerie Web pour effectuer les traitements adéquats sur le message marqué.

Analyse par réputation

L'analyse par liste noire DNS (**RBL)** (*Real time Blackhole List*) permet la qualification d'un message en spam par l'intermédiaire de serveurs RBL. Les menus suivants permettent de configurer la liste des serveurs RBL qui seront utilisés pour cette analyse ainsi que le niveau de confiance accordé à chacun des serveurs.

Liste des serveurs de listes noires DNS (RBL)

Une grille affiche une liste des serveurs RBL auxquels le boîtier UTM envoie ses requêtes pour vérifier qu'un e-mail n'est pas un spam. Cette liste est actualisée par l'« Active Update ». Elle n'est pas modifiable mais vous pouvez toutefois désactiver certains serveurs en cliquant sur la case présente au début de chaque ligne (dans la colonne **Activé**).
Le niveau spécifié dans les colonnes de la grille indique le niveau de confiance accordé à ce serveur.
Vous pouvez aussi configurer vos propres serveurs RBL auxquels vous souhaitez que l'Appliance se connecte. Pour ajouter un serveur, cliquez sur le bouton **Ajouter.** Une nouvelle ligne est ajoutée.
Spécifiez un nom pour ce serveur (unique pour la liste des serveurs RBL), une cible DNS (Champ : **Nom de domaine** uniquement. Cela doit être un nom de domaine valide), un niveau de confiance (Bas, Moyen, Haut) et enfin un commentaire. L'indication du commentaire est facultative. Puis cliquez sur **Appliquer.**
Pour supprimer un serveur configuré, sélectionnez-le dans la liste puis cliquez sur le bouton **Supprimer**.

 **NOTE**
La différenciation entre les serveurs RBL nativement configurés par NETASQ et les serveurs configurés de manière personnalisée s'effectue grâce au cadenas qui indique les serveurs **RBL** nativement configurés par NETASQ.

✪ Rappel : seule la liste de ces serveurs est mise à jour par **Active Update**.

Analyse heuristique

L'analyse heuristique est basée sur l'antispam Vade Retro de GOTO Software. Cet antispam délivre, par un calcul original, un degré de légitimité aux messages.
L'antispam effectue le calcul d'une valeur définissant le caractère « non sollicité » d'un message. Les e-mails obtenant une valeur supérieure ou égale au seuil fixé seront considérés comme spam.

Score minimal de définition d'un spam [1-5000]	L'analyse heuristique réalisée par le module **Antispam** effectue le calcul d'une valeur définissant le caractère "non-sollicité" d'un message. Les e-mails obtenant une valeur supérieure ou égale au seuil fixé seront considérés comme spams. Cette section permet de définir le seuil à appliquer, par défaut NETASQ choisit "200". En modifiant le score, la valeur minimale des 3 seuils de confiance est modifiée. De plus, plus cette valeur calculée est élevée plus le niveau de confiance accordé par l'antispam à l'analyse sera élevé. Les seuils de franchissement des niveaux de confiance ne sont pas configurables dans l'interface d'administration Web.

L'onglet « Domaines en liste blanche»

Cette section permet de définir les domaines en provenance desquels les messages analysés seront systématiquement définis comme **légitimes**. Pour ajouter un domaine à autoriser, référez-vous à la procédure suivante :

Nom de domaine (caractères génériques acceptés : * et ?)	Permet de spécifier le domaine à autoriser. Cliquer sur **Ajouter**. Le domaine ainsi ajouté apparaît alors dans la liste des domaines en liste blanche. Pour supprimer un domaine donné ou la liste complète des domaines, cliquez respectivement sur **Supprimer**.

 **NOTE**
L'antispam ne qualifiera JAMAIS comme Spam les messages provenant des domaines cités dans la liste blanche.

L'onglet « Domaines en liste noire »

Cette section permet de définir les domaines en provenance desquels les messages analysés seront systématiquement définis comme spam. Pour ajouter un domaine à bloquer, référez-vous à la procédure suivante :

Nom de domaine (caractères génériques acceptés : * et ?)	Permet de spécifier le domaine à bloquer. Cliquer sur **Ajouter**. Le domaine ainsi ajouté apparaît alors dans la liste des domaines bloqués. Chaque message identifié comme spam du fait de ces domaines en liste noire seront associés au niveau de confiance le plus élevé (à savoir 3). Pour supprimer un domaine donné ou la liste complète des domaines, cliquez respectivement sur **Supprimer**.

REMARQUES GENERALES

L'antispam qualifiera comme Spam tous les messages provenant des domaines cités dans la liste noire.

Le filtrage par liste blanche et liste noire prévaut sur les méthodes d'analyses par liste noire DNS et analyse heuristique. Le nom de domaine de l'expéditeur est successivement comparé aux domaines en liste noire et liste blanche.
Pour chacune des listes, il est possible de définir jusqu'à 50 domaines. Il n'est pas possible d'avoir dans une liste deux fois le même domaine. Le domaine peut se trouver, soit en liste blanche, soit en liste noire.
Un nom de domaine peut contenir des caractères alphanumériques, "_", "-" et ".". Les caractères "Wildcard" "*" et "?" sont également autorisés. La longueur du nom de domaine ne peut excéder 128 caractères.

ANTIVIRUS

L'écran de configuration du service Antivirus comporte 2 zones :

- Une zone de choix de l'antivirus
- Une zone de paramètres

Moteur antiviral

La liste déroulante permet de migrer entre solutions Antivirus (ClamAV ou Kaspersky). En sélectionnant un antivirus, le message suivant s'affiche :
« *Le changement d'antivirus nécessite le téléchargement complet de la base antivirale. Durant cet intervalle, l'analyse antivirale échouera* ». Cliquez sur **Changer de moteur** pour valider votre choix. Une fois que la base est téléchargée, l'antivirus est activé.

Paramètres

L'analyse des fichiers ClamAV

Dans ce menu, vous configurez les types de fichiers qui doivent être analysés par le service Antivirus du firewall NETASQ.

Analyse des exécutables compressés	Cette option permet d'activer le moteur de décompression (Diet,Pkite, Lzexe, Exepack…).
Analyses des archives	Cette option permet d'activer le moteur d'extraction et d'analyser les archives (zip, arj, lha, rar, cab…)
Bloquer les fichiers protégés par mot de passe	Cette option permet de bloquer les fichiers protégés par mot de passe.
Bloquer les formats de fichiers non supportés.	Cette option permet de bloquer les formats de fichiers que l'antivirus ne peut analyser.

L'analyse des fichiers Kaspersky

Analyse des archives	Cette option permet d'activer le moteur d'extraction et d'analyser les archives (zip, arj, lha, rar, cab…).
Bloquer les fichiers protégés par mot de passe	Cette option permet de bloquer les fichiers protégés par mot de passe.

AUTHENTIFICATION

La fonction d'authentification permet à l'utilisateur de déclarer son login et de s'identifier, en fournissant un mot de passe qu'il est le seul à pouvoir connaître et qui protège ses données personnelles.

Elle utilise une base de données LDAP (*Lightweight Directory Access Protocol*) stockant des fiches utilisateurs et, éventuellement, le certificat numérique x509 de l'utilisateur.

Une fois l'authentification réussie, le login de l'utilisateur est associé à la machine à partir de laquelle celui-ci s'est identifié et à tous les paquets IP qui en proviennent, et ce pour une durée spécifiée par l'utilisateur.

Le module **Authentification** se compose d'un assistant de configuration, disponible en sélectionnant l'icône suivante et comportant plusieurs étapes variables selon l'annuaire que vous y choisirez.
Il est découpé en 4 onglets :

- **Général** : Permet de configurer l'accès au portail captif depuis les différentes interfaces, ainsi que les différentes informations relatives à celui-ci (accès SSL, authentification, proxy).
- **Méthodes disponibles** : Cet onglet vous propose de choisir une ou plusieurs méthodes d'authentification et de les configurer, en précisant si vous souhaitez les autoriser sur les interfaces internes et externes.
- **Interfaces internes** : Permet d'effectuer la gestion des mots de passe des utilisateurs, les durées d'authentification autorisées et l'enrôlement au niveau des interfaces internes.
- **Interfaces externes** : Permet d'effectuer la gestion des mots de passe des utilisateurs, les durées d'authentification autorisées et l'enrôlement au niveau des interfaces externes.

Assistant d'authentification

Cette partie vous permet de choisir votre méthode d'authentification :

- S'authentifier sur un annuaire Active Directory (méthode Kerberos)
- S'authentifier sur l'annuaire interne (méthode LDAP)
- S'authentifier sur une base RADIUS

A partir de la version 9.0.1, les liens ajoutés sur le portail d'authentification en version 9 sont traduits dans toutes les langues supportées.

Les caractères de niveau ISO-8859-15 (« € » inclus) sont autorisés pour le mot de passe des administrateurs.

S'authentifier sur un annuaire Active Directory (méthode Kerberos)

Kerberos diffère des autres méthodes d'authentification. Plutôt que de laisser l'authentification avoir lieu entre chaque machine cliente et chaque serveur, Kerberos utilise un cryptage symétrique, le Centre distributeur de tickets (KDC, Key Distribution Center) afin d'authentifier les utilisateurs sur un réseau.
Dans ce processus d'authentification le boîtier agit comme un client qui se substitue à l'utilisateur pour demander une authentification. Cela signifie que même si l'utilisateur est déjà authentifié sur le KDC pour son ouverture de session Windows par exemple, il faut tout de même se ré-authentifier auprès de ce serveur même si les informations de connexion sont identiques, pour traverser le firewall.

Etape 1 : Interfaces

L'authentification sur les firewalls est différenciée par les interfaces sur lesquelles arrivent les flux de trafic.
Il est possible d'activer l'authentification depuis les interfaces internes, depuis les interfaces externes ou depuis les deux types d'interfaces.

Autoriser les utilisateurs à s'authentifier :

Depuis les réseaux internes (interfaces protégées)	Si cette option est cochée, l'identification est rendue possible depuis les interfaces protégées à l'intérieur de l'entreprise, matérialisées par l'icône .
Depuis les réseaux publics (interfaces externes – nécessaire pour le VPN SSL)	Il est possible de s'identifier sur les firewalls depuis les interfaces non protégées. Vous pouvez par exemple, vous connecter sur un firewall depuis votre domicile, en passant par le VPN SSL (Voir module `VPN\VPN SSL`).
Depuis les réseaux internes et publics	En cochant cette case, l'authentification sera possible depuis n'importe quelle interface.

Etape 2 : Méthodes d'authentification

Si vous choisissez de vous authentifier sur un annuaire Active Directory, cochez la case correspondante et cliquez sur **Suivant**.

Etape 3 : Méthode Kerberos

Accès au serveur Active Directory (méthode Kerberos)

Nom de domaine (Kerberos)	Nom de domaine attribué au serveur Active Directory pour la méthode d'authentification Kerberos.
Serveur	Vous devez choisir un objet correspondant à votre serveur Active Directory au sein de la liste déroulante affichée.


REMARQUE
Vous allez sauter l'**Etape 4** de la configuration, relatives à la **Gestion des mots de passe**, car la méthode d'authentification Kerberos ne nécessite pas de configuration spécifique pour cela.

Etape 5 : Résumé

Configuration de l'authentification

Cet écran vous permet de finaliser la configuration de l'authentification que vous venez d'effectuer.
Pour Kerberos, l'encadré récapitulatif contient :
- Le nom de(s) l'interface(s) depuis laquelle l'authentification est autorisée.
- La méthode d'authentification utilisée
- Le nom de domaine Kerberos
- Le nom du serveur attribué

Si ces informations vous conviennent, vous pouvez cliquer sur **Terminé.**

S'authentifier sur l'annuaire interne (méthode LDAP)

Etape 1 : Interfaces

Autoriser les utilisateurs à s'authentifier :

Depuis les réseaux internes (interfaces protégées)	Si cette option est cochée, l'identification est rendue possible depuis les interfaces protégées à l'intérieur de l'entreprise, matérialisées par l'icône . Celles-ci figurent dans le LAN, définissant le réseau local, ou un ensemble de machine appartenant à une même organisation. (« In », « Dmz » etc.).
Depuis les réseaux publics (interfaces externes – nécessaire pour le VPN SSL)	Il est possible de s'identifier sur les firewalls depuis les interfaces non protégées. Vous pouvez par exemple, vous connecter sur un firewall depuis votre domicile, en passant par le VPN SSL (Voir module `VPN\VPN SSL`).
Depuis les réseaux internes et publics	En cochant cette case, l'authentification sera possible depuis n'importe quelle interface.

Etape 2 : Méthodes d'authentification

Si vous choisissez de vous authentifier sur l'annuaire interne (méthode LDAP), cochez la case correspondante et cliquez sur **Suivant**.

Etape 3 : Enrôlement des utilisateurs

Autoriser l'accès au portail captif et l'enrôlement depuis les réseaux protégés (interfaces internes)	En cochant cette option, vous activez l'authentification sur les interfaces internes, et vous permettez aux utilisateurs inconnus à votre annuaire, de s'inscrire et de remplir un formulaire de demande de création de compte.  **NOTE** Lors de la création d'un nouvel utilisateur, la méthode de hachage SHA sera utilisée pour le stockage des mots de passe, par défaut.

Etape 4 : Gestion des mots de passe

Les utilisateurs ne peuvent pas changer leur mot de passe	En sélectionnant cette option, il sera impossible aux utilisateurs de modifier leur mot de passe d'authentification sur le firewall NETASQ.
Les utilisateurs peuvent changer leur mot de passe	En cochant cette case, les utilisateurs peuvent modifier leur mot de passe d'authentification sans contrainte de temps et de validité.
Les utilisateurs doivent changer leur mot de passe	En sélectionnant cette option, les utilisateurs doivent changer leur mot de passe d'authentification à leur première connexion sur le portail d'authentification du firewall puis à chaque fois que la durée de validité du mot de passe est expiré. Cette durée est spécifiée en jours. Un champ intitulé **Durée de vie** apparait au-dessous, vous permettant d'indiquer le nombre de jours de validité du mot de passe.

Etape 5 : Résumé

Configuration de l'authentification

Cet écran vous permet de finaliser la configuration de l'authentification que vous venez d'effectuer.
Pour l'annuaire interne, l'encadré récapitulatif contient :
- Le nom de(s) l'interface(s) depuis laquelle l'authentification est autorisée.
- La méthode d'authentification utilisée
- L'état de l'option d'enrôlement (**Active** ou **Inactive**)
- Le type de gestion des mots de passe choisi (Voir *Etape 4*)

Si ces informations vous conviennent, vous pouvez cliquer sur **Terminé.**

S'authentifier sur une base RADIUS

RADIUS est un protocole d'authentification standard, fonctionnant en mode client-serveur. Il permet de définir les accès réseau à des utilisateurs distants. Ce protocole est doté d'un serveur relié à une base d'identification (annuaire LDAP etc.) Le firewall NETASQ peut se comporter comme un client RADIUS. Il peut alors adresser, à un serveur RADIUS externe, des demandes d'authentification pour les utilisateurs désirant traverser le firewall. L'utilisateur ne sera authentifié que si le RADIUS accepte la demande d'authentification envoyée par le firewall.

Toutes les transactions RADIUS (communications entre le firewall et le serveur RADIUS) sont elles-mêmes authentifiées par l'utilisation d'un secret pré-partagé, qui n'est jamais transmis sur le réseau. Ce même secret sera utilisé pour chiffrer le mot de passe de l'utilisateur, qui transitera entre le firewall et le serveur RADIUS.

Etape 1 : Interfaces

Autoriser les utilisateurs à s'authentifier :

Depuis les réseaux internes (interfaces protégées)	Si cette option est cochée, l'identification est rendue possible depuis les interfaces protégées à l'intérieur de l'entreprise, matérialisées par l'icône .
Depuis les réseaux publics (interfaces externes – nécessaire pour le VPN SSL)	Il est possible de s'identifier sur les firewalls depuis les interfaces non protégées. Vous pouvez par exemple, vous connecter sur un firewall depuis votre domicile, en passant par le VPN SSL (Voir module `VPN\VPN SSL`).
Depuis les réseaux internes et publics	En cochant cette case, l'authentification sera possible depuis n'importe quelle interface.

Etape 2 : Méthodes d'authentification

Si vous choisissez de vous authentifier sur une base RADIUS, cochez la case correspondante et cliquez sur **Suivant**.

Etape 3 : Serveur Radius

Accès à la base RADIUS :

Serveur	Vous devez choisir un objet correspondant à votre serveur RADIUS au sein de la liste déroulante affichée.
Clé prépartagée	Mot de passe permettant d'accéder au serveur de votre base RADIUS.

Etape 5 : Résumé

Configuration de l'authentification

Cet écran vous permet de finaliser la configuration de l'authentification que vous venez d'effectuer.
Pour la base RADIUS, l'encadré récapitulatif contient :
- Le nom de(s) l'interface(s) depuis laquelle l'authentification est autorisée.
- La méthode d'authentification utilisée
- Le nom du serveur
- La clé prépartagée affichée en clair

Si ces informations vous conviennent, vous pouvez cliquer sur **Terminé.**

Onglet « Général »

Activer le portail captif

En cochant cette option, vous activez le module `Authentification` et autorisez l'authentification via un formulaire web depuis les interfaces protégées et/ou publiques.
Vous pouvez précisez depuis quelle(s) interface(s) vous souhaitez autoriser l'accès en cochant l'un des champs suivants :

Uniquement depuis les interfaces internes (protégées)	Si cette option est cochée, l'identification est uniquement possible depuis les interfaces protégées à l'intérieur de l'entreprise, matérialisées par l'icône .
Uniquement depuis les interfaces externes (publiques)	Il ne sera possible de s'identifier sur les firewalls seulement depuis les interfaces non protégées. Vous pouvez par exemple, vous connecter sur un firewall depuis votre domicile, en passant par le VPN SSL (Voir module `VPN\VPN SSL`).
Depuis les interfaces internes et externes	En cochant cette case, l'authentification sera possible depuis n'importe quelle interface.


REMARQUE
Si la case **Activer le portail captif** n'est pas cochée, les champs ci-dessus seront grisés.

Portail captif : accès SSL

Certificat (clé privée)	Par défaut la CA utilisée par le module d'authentification du firewall est la CA propre du firewall, le nom associé à cette CA est le numéro de série du produit. Ainsi lorsqu'un utilisateur essaie de contacter le firewall différemment que par son numéro de série, il reçoit un message d'avertissement indiquant une incohérence entre ce que l'utilisateur essaie de contacter et le certificat qu'il reçoit. En cliquant sur le bouton l'icône , l'écran de configuration des CA s'affiche (certificat serveur).

Configuration avancée

Authentification des utilisateurs

Ce champ va permettre de personnaliser l'identification en cochant différentes options :

Interrompre les connexions lorsque l'authentification expire	Dès que la durée de vie de l'authentification arrive à échéance les connexions seront interrompues même si l'utilisateur est en cours de téléchargement
Utiliser le compte du firewall pour vérifier l'authentification des utilisateurs sur l'annuaire	En cochant cette option, le firewall se connecte à la base LDAP interne afin de vérifier les données des utilisateurs.
S'authentifier avec le compte utilisateur directement sur l'annuaire	L'utilisateur se connecte lui-même à l'annuaire en passant à travers le firewall, il renseigne son identifiant et son mot de passe.
Utiliser le nom du firewall comme FQDN	Cette option permet de faire la correspondance entre le numéro de série du Firewall et son adresse IP.

Fichier de configuration du proxy (.pac) :

Ce champ permet d'envoyer au firewall le fichier .PAC à distribuer qui représente le fichier de configuration automatique du proxy (Proxy Auto-Config). L'utilisateur peut récupérer un fichier PAC ou alors vérifier son contenu à l'aide du bouton situé à droite du champ.
L'utilisateur peut spécifier dans son navigateur web, le script de configuration automatique qui se situe dans https://if_firewall>/config/wpad.dat.

Portail captif

Masquer le logo NETASQ	Cette option donne la possibilité de ne pas faire apparaître la bannière NETASQ lors de l'authentification de l'utilisateur sur le portail captif, par souci de confidentialité.

Onglet « Méthodes disponibles »

Cet onglet se décompose en 3 parties :

- La colonne de gauche dédiée aux méthodes d'authentification, englobant les interfaces autorisées.
- La colonne de droite affichant les options de paramétrage de la méthode d'authentification sélectionnée.
- Le champ de méthode de redirection du proxy HTTP.

Méthodes d'authentification

Le bouton **Ajouter une méthode d'authentification** ouvre une liste déroulante vous proposant de choisir parmi 5 méthodes d'authentification, que vous pourrez **Supprimer** si besoin :

LDAP

La configuration de cette méthode est automatique et nécessite l'implémentation d'une base LDAP, vous devez vous rendre dans le menu `Utilisateurs\Configuration de l'annuaire` pour y accéder.

Certificat (SSL)

Après avoir sélectionné votre méthode d'authentification dans la colonne de gauche, vous pouvez saisir ses informations dans la colonne de droite, qui présente les éléments suivants :

Autorités de confiance (C.A)

La méthode d'authentification SSL peut accepter l'utilisation de certificats signés par une autorité de certification externe au firewall. Pour cela il est nécessaire d'ajouter cette autorité de certification dans la configuration du firewall de façon à ce que celui accepte tous les certificats effectivement signés par cette autorité.
Si l'autorité de certification est elle-même signée par une autre autorité de certification, il est possible de rajouter cette autorité dans la liste des CA de confiance pour ainsi créer une "Chaîne de confiance".

Lorsqu'une CA de confiance ou une chaîne de CA de confiance est spécifiée dans la configuration de la méthode d'authentification SSL, elle s'ajoute à la CA interne du firewall implicitement vérifiée dès qu'il existe une autorité racine interne valide sur le firewall.

Ajouter	L'ajout d'une autorité de certification dans la liste des autorités de certification de confiance permet d'accepter cette autorité comme autorité reconnue et de valider tous les certificats signés par cette autorité de certification. En cliquant sur le bouton **Ajouter** on accède à la fenêtre des CA (Cf. *Certificats et PKI*). Si l'autorité de certification à laquelle vous désirez faire confiance ne fait pas partie de la liste des certificats externes, cliquez sur le bouton **Sélectionner** de la fenêtre des certificats externes pour ajouter cette autorité de certification dans la liste. Les firewalls supportent les autorités racines multi niveaux. Ainsi si le certificat de l'utilisateur à authentifier est signé par une autorité de certification, elle-même signée par une autorité de certification supérieure. Vous pouvez insérer toute la chaine de certification créée par cette autorité racine multi niveaux. Pour que toute la chaîne soit correctement prise en compte, il est important d'insérer l'ensemble de la chaîne des autorités entre l'autorité la plus haute que vous avez inséré et l'autorité directement supérieure au certificat utilisateur.
Supprimer	Supprime l'autorité de certification sélectionnée.

Autorité de certification (C.A) : Ce champ laisse apparaître les certificats auxquels vous faites confiance et que vous serez amenés à utiliser.

A partir de la version 9.0.1, il est possible de modifier le champ du sujet du certificat qui sera utilisé pour rechercher l'utilisateur dans le LDAP. Il est également possible de modifier le champ LDAP utilisé pour la recherche. Par défaut, l'e-mail est utilisé dans les deux cas. Ces paramètres sont configurables via la CLI.

RADIUS

Après avoir sélectionné votre méthode d'authentification dans la colonne de gauche, vous pouvez saisir ses informations dans la colonne de droite, qui présente les éléments suivants :

Accès au serveur

Lorsque la méthode RADIUS est sélectionnée, l'authentification RADIUS est activée. Ce menu vous permet de préciser les informations relatives au serveur RADIUS externe utilisé et d'un éventuel serveur RADIUS de sauvegarde. Pour chacun la configuration nécessite de renseigner les informations présentées dans le tableau suivant :

Serveur	Adresse IP du serveur RADIUS.
Port	Port utilisé par le serveur RADIUS, si le serveur principal tombe.
Clé prépartagée	Clé utilisée pour le chiffrement des échanges entre le firewall et le serveur RADIUS.

Serveur de rechange

Serveur	Adresse IP du serveur de rechange.
Port	Port utilisé pour le serveur de rechange, si le serveur principal tombe.
Clé prépartagée	Clé utilisée pour le chiffrement des échanges entre le firewall et le serveur de rechange.

REMARQUE
Le firewall tente de se connecter 2 fois au serveur RADIUS "principal", en cas d'échec il tente de se connecter 2 fois au serveur RADIUS "backup". Si le serveur RADIUS "backup" répond, il bascule en tant que serveur RADIUS "principal". Au bout de 600 secondes, un nouveau basculement s'opère, l'ancien serveur RADIUS "principal" redevient "principal".

Kerberos

Après avoir sélectionné votre méthode d'authentification dans la colonne de gauche, vous pouvez saisir ses informations dans la colonne de droite, qui présente les éléments suivants :

Nom de domaine (FQDN)	Nom de domaine attribué au serveur Active Directory pour la méthode d'authentification Kerberos. La définition de ce nom de domaine permet de masquer l'adresse IP du serveur et d'en simplifier la recherche. Exemple : *www.netasq.com* : ***netasq.com*** représente le nom de domaine, plus lisible son adresse IP correspondante : 91.212.116.100.

Accès au serveur

Serveur	Adresse IP du serveur pour la méthode d'authentification Kerberos (*Active Directory* par exemple)
Port	Port utilisé par le serveur.

Serveur de rechange

Serveur	Adresse IP de rechange du serveur Active Directory pour la méthode d'authentification Kerberos.
Port	Port utilisé pour le serveur de rechange

Authentification transparente (SPNEGO)

La méthode SPNEGO permet le fonctionnement du "Single Sign On" pour l’authentification Web avec un serveur d’authentification externe Kerberos. Cela signifie qu’un utilisateur se connectant à son domaine par une solution basée sur un serveur Kerberos serait automatiquement authentifié sur un firewall NETASQ dans le cas d’un accès à l’Internet (nécessitant une authentification dans la politique de filtrage sur le firewall) grâce à un navigateur Web (Internet Explorer, Firefox, Mozilla).

La configuration de SPNEGO sur le firewall est réalisée grâce aux options expliquées dans le tableau suivant :

Nom du service	Il est recommandé d’indiquer le numéro de série du firewall plutôt que son nom pour l’identifier (Ce nom correspond au nom indiqué dans le script NETASQ livré avec le matériel d’installation). Le numéro de série sera précédé de la mention « HTTP/ ». **Exemple** HTTP/U70XXAZ0899020
Nom de domaine	Nom de domaine du serveur Kerberos. Il correspond au nom complet du domaine Active Directory et doit être écrit en majuscules.
KEYTAB	Ce champ représente le secret partagé, généré lors de l'utilisation du script sur l'Active Directory. Ce secret doit être fourni au firewall afin qu'il puisse communiquer avec l'Active Directory. Vous devez exécuter le script de génération de KEYTAB : ***spnego.bat*** en respectant scrupuleusement la casse. Ce script est disponible sur le site web NETASQ ou dans le CD ROM d’administration de votre firewall.

Interfaces autorisés

Interne	Permet d’activer ou de désactiver la méthode d’authentification choisie sur l’interface interne.
Externe	Permet d’activer ou de désactiver la méthode d’authentification choisie sur l’interface externe.


REMARQUE

L’activation de ces champs ajoute la méthode d’authentification sélectionnée à la liste déroulante de la colonne **Authentification** du menu `Utilisateurs\Droits d’accès`\ onglet `Configuration par l’utilisateur.`

Méthodes de redirection du proxy HTTP

Lorsqu’une méthode de redirection par défaut du proxy HTTP est activée (SRP, Certificat ou SPNEGO), le mode SSO de cette méthode est enclenché. Cela signifie que, une fois que vous avez saisi une fois vos identifiant/mot de passe, vous n’aurez plus besoin de vous identifier lors de votre prochaine connexion, ils seront déjà stockés et automatiquement pris en compte.

Interfaces internes	Ce champ nécessite de définir une méthode d’authentification SSL et SPNEGO, et de choisir celle qu’il faut appliquer pour le proxy http vers les interfaces internes.
Interfaces externes	Ce champ nécessite de définir une méthode d’authentification SSL et SPNEGO, et de choisir celle qu’il faut appliquer pour le proxy http vers les interfaces externes.

Onglet « Interfaces internes »

Mots de passe des utilisateurs

Les utilisateurs ne peuvent pas changer leur mot de passe	En sélectionnant cette option, il sera impossible aux utilisateurs de modifier leur mot de passe d'authentification sur le firewall NETASQ.
Les utilisateurs peuvent changer leur mot de passe	En cochant cette case, les utilisateurs peuvent modifier leur mot de passe d'authentification sans contrainte de temps et de validité.
Les utilisateurs doivent changer leur mot de passe	En sélectionnant cette option, les utilisateurs doivent changer leur mot de passe d'authentification à leur première connexion sur le portail d'authentification du firewall puis à chaque fois que la durée de validité du mot de passe est expiré. Cette durée est spécifiée en jours sans précision d'heure. Un champ intitulé **Durée de vie** apparait au-dessous, vous permettant d'indiquer le nombre de jours de validité du mot de passe. **NOTE** Si la durée de validité du mot de passe de l'utilisateur est de 1 jour et que le mot de passe de l'utilisateur est initialisé une première fois le 25 novembre 2010 14:00, ce mot de passe doit être modifié dès le 26 novembre 2010 00:00 et non 24 heures plus tard.

Durées d'authentification autorisées

Durée minimale	Durée minimale durant laquelle l'utilisateur peut être authentifié, positionnable en minutes ou en heures (jusqu'à 24h).
Durée maximale	Durée maximale durant laquelle l'utilisateur peut être authentifié positionnable en minutes ou en heures (jusqu'à 24h).
Pour l'authentification transparente	Cette méthode d'authentification basée sur SSO (Single Sign On-authentification unique) permet de définir la durée pendant laquelle aucune réauthentification transparente ne sera demandée par le firewall.

Configuration avancée

Autoriser l'accès au fichier .PAC depuis les interfaces internes	En cochant cette option, vous autorisez la publication du fichier .PAC sur les interfaces internes. La publication du fichier .PAC est également possible pour les interfaces externes.

Enrôlement des utilisateurs

NETASQ vous propose l'enrôlement d'utilisateurs par le web. Si l'utilisateur qui tente de se connecter ne figure pas dans la base des utilisateurs, il a la possibilité de demander la création de son compte par un enrôlement Web.

Ne pas permettre l'enrôlement des utilisateurs	Si cette case est cochée, aucun utilisateur « inconnu » à l'annuaire LDAP ne pourra s'y inscrire ni créer de compte.
Autoriser l'enrôlement web des utilisateurs	La création d'un compte utilisateur doit être effectuée pour que cette option soit fonctionnelle. Si cette case est cochée, tout utilisateur tentant de se connecter et ne figurant pas dans la base des utilisateurs aura la possibilité de demander la création de son compte en remplissant un formulaire web. La demande pourra être validée ou refusée par un administrateur.
Autoriser l'enrôlement web des utilisateurs et créer leur certificat	Si cette option est activée, vous pourrez non seulement demander la création de votre compte si vous ne figurez pas dans la base des utilisateurs, mais aussi demander la création d'un certificat.

Notification d'un nouvel enrôlement

Cette option permet d'avertir les nouveaux enrôlés de la création de leur compte dans la base utilisateurs.

Pas d'email envoyé	Par défaut, la liste déroulante affiche qu'aucun email de sera envoyé à l'administrateur pour le prévenir d'une demande d'enrôlement. Vous pouvez en outre, définir un groupe d'utilisateurs auquel les demandes d'enrôlement seront transmises dans le menu `Notifications\Alertes e-mails\ onglet Destinataires`. Une fois créé, ce groupe sera automatiquement inclus au sein de la liste déroulante et pourra recevoir les requêtes si vous le sélectionnez.

Association utilisateur/adresse IP

Autoriser plusieurs utilisateurs à être authentifiés depuis la même adresse IP	En cochant cette option, il est possible d'enregistrer plusieurs logins sur la même adresse IP. L'adresse réelle des utilisateurs est masquée par une adresse IP unique. (voir Module **`Politique de Sécurité\Filtrage et NAT`**).
Interdire l'authentification simultanée d'un utilisateur sur plusieurs machines	Cette option permet d'éviter qu'un utilisateur ne s'identifie sur plusieurs postes en même temps. En l'activant, ses requêtes multiples seront automatiquement refusées.

Expiration du 'cookie' HTTP

La gestion des cookies pour l'authentification des utilisateurs sur les firewalls permet une sécurisation de l'authentification prévenant par exemple les attaques par rejeu étant donné qu'il est indispensable de posséder le cookie de connexion pour être considéré comme authentifié.

Les cookies sont indispensables pour le fonctionnement de l'option **Autoriser plusieurs utilisateurs à être authentifiés depuis la même adresse IP**.
Ils sont négociés par navigateur Web. Ainsi si une authentification est réalisée avec Internet Explorer, elle ne sera pas effective avec Firefox ou d'autres navigateurs Web.

A la fin de la période d'authentification	Par défaut le cookie HTTP expire **A la fin de la période d'authentification,** ce qui signifie qu'il n'est négocié qu'une seule fois pour toute la durée d'authentification.
A la fin de la session	Le cookie sera négocié à chaque requête vers votre navigateur web.
Ne pas utiliser (déconseillé)	Il est possible de ne pas utiliser de cookie HTTP, mais cette option n'est pas recommandée car elle dégrade la sécurité de l'authentification.

Onglet « Interfaces externes »

Mots de passe des utilisateurs

Les utilisateurs ne peuvent pas changer leur mot de passe	En sélectionnant cette option, il sera impossible aux utilisateurs de modifier leur mot de passe d'authentification sur le firewall NETASQ.
Les utilisateurs peuvent changer leur mot de passe	En cochant cette case, les utilisateurs peuvent modifier leur mot de passe d'authentification sans contrainte de temps et de validité.
Les utilisateurs doivent changer leur mot de passe	En sélectionnant cette option, les utilisateurs doivent changer leur mot de passe d'authentification à leur première connexion sur le portail d'authentification du firewall puis à chaque fois que la durée de validité du mot de passe est expiré. Cette durée est spécifiée en jours. Un champ intitulé **Durée de vie** apparait au-dessous, vous permettant d'indiquer le nombre de jours de validité du mot de passe.

Durées d'authentification autorisées

Durée minimale	Durée minimale durant laquelle l'utilisateur peut être authentifié, positionnable en minutes ou en heures (jusqu'à 24h).
Durée maximale	Durée maximale durant laquelle l'utilisateur peut être authentifié positionnable en minutes ou en heures (jusqu'à 24h).
Pour l'authentification transparente	Cette méthode d'authentification basée sur SSO (Single Sign On-authentification unique) permet de définir la durée pendant laquelle aucune réauthentification transparente ne sera demandée par le firewall.

Configuration avancée

Autoriser l'accès au fichier .PAC depuis les interfaces internes	En cochant cette option, vous autorisez la publication du fichier .PAC sur les interfaces internes. La publication du fichier .PAC est également possible pour les interfaces externes.

Enrôlement des utilisateurs

Ne pas permettre l'enrôlement des utilisateurs	Si cette case est cochée, aucun utilisateur « inconnu » à l'annuaire LDAP ne pourra s'y inscrire ni créer de compte.
Autoriser l'enrôlement web des utilisateurs	La création d'un compte utilisateur doit être effectuée pour que cette option soit fonctionnelle. Si cette case est cochée, tout utilisateur tentant de se connecter et ne figurant pas dans la base des utilisateurs aura la possibilité de demander la création de son compte en remplissant un formulaire web. La demande pourra être validée ou refusée par un administrateur.
Autoriser l'enrôlement web des utilisateurs et créer leur certificat	Si cette option est activée, vous pourrez non seulement demander la création de votre compte si vous ne figurez pas dans la base des utilisateurs, mais aussi demander la création d'un certificat.

Notification d'un nouvel enrôlement

Pas d'email envoyé	Par défaut, la liste déroulante affiche qu'aucun email de sera envoyé à l'administrateur pour le prévenir d'une demande d'enrôlement. Vous pouvez en outre, définir un groupe d'utilisateurs auquel les demandes d'enrôlement seront transmises dans le menu `Notifications\Alertes e-mails\ onglet Destinataires.` Une fois créé, ce groupe sera automatiquement inclus au sein de la liste déroulante et pourra recevoir les requêtes si vous le sélectionnez.

Association utilisateur/adresse IP

Autoriser plusieurs utilisateurs à être authentifiés depuis la même adresse IP	En cochant cette option, il est possible d'enregistrer plusieurs logins sur la même adresse IP. L'adresse réelle des utilisateurs est masquée par une adresse IP unique. (voir Module **`Politique de Sécurité\Filtrage et NAT`**).
Interdire l'authentification simultanée d'un utilisateur sur plusieurs machines	Cette option permet d'éviter qu'un utilisateur ne s'identifie sur plusieurs postes en même temps. En l'activant, ses requêtes multiples seront automatiquement refusées.

Expiration du 'cookie' HTTP

A la fin de la période d'authentification	Par défaut le cookie HTTP expire A la fin de la période d'authentification, ce qui signifie qu'il n'est négocié qu'une seule fois pour toute la durée d'authentification.
A la fin de la session	Le cookie sera négocié à chaque requête vers votre navigateur web.
Ne pas utiliser (déconseillé)	Il est possible de ne pas utiliser de cookie HTTP, mais cette option n'est pas recommandée car elle dégrade la sécurité de l'authentification.

CERTIFICATS ET PKI

La PKI ou *Public Key Infrastructure* (infrastructure à clé publique) est un système cryptographique (basé sur la cryptographie asymétrique). Elle utilise des mécanismes de signature et certifie des clés publiques qui permettent, par exemple, de chiffrer et de signer des messages ou des flux de données. Elle permet d'assurer confidentialité, authentification, intégrité et non-répudiation.

La PKI NETASQ permet de générer et de délivrer des autorités de confiance (CA : *Certificate Authority,* ou « autorité de certification ») ainsi que des certificats. Ceux-ci contenant une bi-clé associée à des informations pouvant appartenir à un utilisateur, un serveur etc. La PKI NETASQ a pour objectif d'authentifier ces éléments.

L'écran du module `Certificats et PKI` se divise en 3 parties :

- En haut de l'écran, les différentes actions possibles sous formes d'une barre de recherche et de boutons.
- A gauche, la liste des autorités et des certificats.
- A droite, les détails concernant l'autorité ou le certificat sélectionné au préalable dans la liste de gauche, ainsi que les informations concernant la CRL et la configuration de La CA ou sous CA.

Les actions possibles

La barre de recherche

Si vous recherchez un certificat ou une CA existante en particulier, saisissez son nom.
Le champ de recherche vous permet de lister tous les certificats et les CA dont le nom correspond aux mots clés saisis.
Exemple :
Si vous saisissez la lettre « a » dans la barre de recherche, la liste en dessous fera apparaître tous les certificats possédant un « a ».

Le filtre

Ce bouton permet de choisir le type de certificat à afficher et de ne voir que les éléments qui vous intéressent. Un menu déroulant vous propose les choix suivants :

Tous	Matérialisé par l'icône, cette option permet d'afficher dans la liste de gauche, toutes les autorités et certificats préalablement créés.
Autorités	Matérialisé par l'icône, cette option permet d'afficher dans la liste de gauche, toutes les autorités et sous-autorités.
Certificats utilisateur	Matérialisé par l'icône, cette option permet d'afficher uniquement les certificats utilisateur et les CA dont ils dépendent.
Certificats serveur	Matérialisé par l'icône, cette option permet d'afficher uniquement les certificats serveur et les CA dont ils dépendent.
Certificats Smartcard	Matérialisé par l'icône, cette option permet d'afficher uniquement les certificats Smartcard et les CA dont ils dépendent.

Ajouter

L'écran du module `Certificats et PKI` propose d'**Ajouter** différents types d'autorités :
Pour chacune d'entre elles, une fenêtre d'assistant s'affichera afin de définir les propriétés de l'autorité.

A partir de la version 9.0.1, vous pouvez ajouter des CRLDP (points de distribution des CRL) pour les CA importées via le GUI.

Assistant d'ajout d'autorités et de certificats

Le bouton **Ajouter** déroule une liste proposant 6 actions permettant de créer une autorité ou un certificat, par le biais d'un assistant.

Ajouter une autorité racine

Une autorité racine ou « root CA » est une entité ayant pour objectif de signer, émettre et maintenir les certificats et les CRL (*Certificate Revocation List* ,ou « listes de révocations »).

Vous devez définir les propriétés de l'autorité que vous souhaitez ajouter :



Ces informations ne seront plus modifiables après leur création.

CN	Saisissez un nom permettant d'identifier votre autorité racine, dans la limite de 64 caractères maximum. Ce nom peut faire référence à une organisation, un utilisateur, un serveur, une machine etc. **Exemple** *NETASQ*  **NOTE** Ce champ doit être rempli afin de poursuivre la configuration.
Identifiant	Bien que le remplissage de ce champ ne soit pas obligatoire, vous pouvez ici indiquer un raccourci de votre CN, utile pour vos lignes de commande. **Exemple** Si vous aviez choisi un nom et un prénom pour votre CN, l'identifiant peut en indiquer les initiales uniquement.

<u>Sélectionnez l'autorité parente (si nécessaire)</u>

Choisir une autorité parente implique le pré-remplissage des attributs de l'autorité dans les champs du dessous.

Autorité parente	Bien qu'une CA ou autorité de certification soit composée de certificats, elle peut également impliquer des sous CA qui dépendent d'elle. L'utilisation d'une sous CA n'est possible qu'après identification de son « **Autorité parente** » ou CA.
Mot de passe autorité parente	Définissez un mot de passe si vous souhaitez notifier que vous êtes bien responsable de la CA parente.

Attributs de l'autorité

Lors de cette étape, vous devez renseigner les informations générales concernant l'autorité que vous voulez mettre en œuvre. Les informations saisies se retrouveront dans le certificat de votre autorité de certification et dans les certificats de vos utilisateurs.



Dans le cas d'une sous CA ces données sont pré-remplies. Et à moins de modifier la configuration, il n'est pas possible de tous les modifier.

Organisation (O)	Nom de votre société (ex : NETASQ).
Unité d'organisation (OU)	"branche" de votre société (ex : INTERNE).
Lieu (L)	Ville dans laquelle est située votre société (ex : Villeneuve d'Ascq).
Etat ou province (ST)	Département géographique de votre société (ex : Nord).
Pays (C)	Choisissez dans la liste le pays de la société (ex : France).

Cliquer sur **Suivant**.
Vous devez ensuite sécuriser l'accès à votre autorité.
Dans cette étape de l'assistant de configuration de la PKI, vous devez renseigner un mot de passe qui va permettre la protection de la clé privée de votre autorité de certification.



Le choix d'un mot de passe trop simple est déconseillé. Nous vous recommandons de mélanger les lettres minuscules, majuscules, les chiffres, les caractères spéciaux.

Mot de passe de l'autorité

Mot de passe (8 car.min.)	Saisissez un mot de passe de 8 lettres minimum afin de protéger l'accès à votre CA. **NOTE** Ce mot de passe ne sera pas enregistré par le firewall. Si vous l'oubliez, vous devrez réinitialiser la PKI et perdrez la configuration effectuée pour celle-ci.
Confirmez le mot de passe	Retapez une seconde fois votre mot de passe dans ce champ afin de le confirmer.
Force du mot de passe	Ce champ indique le niveau de sécurité de votre mot de passe : « Très Faible », « Faible », « Moyen », « Bon » ou « Excellent ». Il est fortement conseillé d'utiliser les majuscules et les caractères spéciaux.

E-mail :

Renseigner votre adresse e-mail dans ce champ vous permettra de recevoir un message vous confirmant la création de votre autorité.

Taille de clé (octets)

Lorsque vous créez une CA, vous devez fournir une clé sous forme d'un mot de passe afin de permettre le chiffrage du trafic. Plus la taille de la clé est grande, plus la sécurité est importante.
4 tailles de clés en octets vous sont proposées :

1024	Si vous choisissez cette taille de clé, le mot de passe généré pour votre autorité aura une taille de 1024 octets. **NOTE** Ce nombre correspond à 1024 caractères visibles au sein de la console de votre poste.
1536	Si vous choisissez cette taille de clé, le mot de passe généré pour votre autorité aura une taille de 1536 octets.
2048	Si vous choisissez cette taille de clé, le mot de passe généré pour votre autorité aura une taille de 2048 octets.
4096	Si vous choisissez cette taille de clé, le mot de passe de votre autorité ne devra pas excéder 4096 octets. **AVERTISSEMENT** Bien que les clés de grande taille soient plus efficaces, il est déconseillé d'utiliser celle-ci avec les équipements d'entrée de gamme, comme le U30 ; et ce, pour des raisons de temps de génération.

NOTE
Le calcul des clés de grande taille peut provoquer le ralentissement de votre équipement NETASQ lors de la génération.

Validité (jours)

Ce champ correspond au nombre de jours durant lesquels votre certificat d'autorité et par conséquent votre PKI seront valides. Cette date influe sur tous les aspects de votre PKI, en effet, une fois ce certificat expiré, tous les certificats utilisateurs le seront également. Cette valeur ne sera pas modifiable par la suite.



NOTE
La valeur de ce champ de doit pas excéder 3650 jours.

Cliquez sur **Suivant**.

Dans cette étape de l'assistant, vous devez renseigner la configuration concernant la distribution de la CRL (*Certification Revocation List*) ou liste des certificats révoqués. Cette information sera intégrée aux CA générées et permettra aux applications utilisant le certificat de récupérer automatiquement la CRL afin de vérifier la validité du certificat.

Vous pouvez à présent gérer vos révocations de certificats au sein de la grille qui apparaît à l'écran et entrer les URL faisant office de points de distribution de certificats révoqués (invalides).

Ajouter	En cliquant sur ce bouton, une ligne vierge s'affiche et permet d'entrez une URL comme point de distribution des listes de révocations de certificats. Le première URL que vous inscrirez sera numérotée « 1 » et ainsi de suite. Le firewall va traiter les éléments de la CRL selon leur ordre d'apparition à l'écran.
Supprimer	Placez-vous sur la ligne à supprimer et cliquez sur ce bouton pour l'enlever de la liste.
Monter	Faites remonter votre URL d'une ligne dans l'ordre de priorité de la grille en cliquant sur ce bouton. Renouvelez l'opération plusieurs fois selon le numéro que vous souhaitez donner à

	votre URL.
Descendre	Faites descendre d'une ou plusieurs places votre URL dans la liste en cliquant sur ce bouton.

La fenêtre suivante présente un résumé des informations de votre certificat.
Cliquez sur **Terminer**.

Vous verrez désormais apparaître, au sein de la colonne de gauche de l'écran `Certificats et PKI` la CA que vous venez de créer, matérialisée par l'icône suivante (qui représente la CA par défaut).

En cliquant sur la CA concernée, ses informations détaillées s'afficheront à droite de l'écran en 3 onglets :

L'onglet « Détails »

4 fenêtres y reprennent les données concernant, la « **Validité** » de l'autorité, son destinataire (« **Emis pour** »), son « **Emetteur** » et ses « **Empreintes** » (informations sur la CA et sa version).

L'onglet « CRL »

Il reprend les informations concernant la CRL : la validité incluant la dernière et la prochaine mise à jour, la grille des points de distribution et la grille de certificats révoqués, devant contenir un numéro de série, une date de révocation et un motif de révocation (facultatif).

A partir de la version 9.0.1, la durée de vie maximum des certificats équivaut à dix ans.

L'onglet configuration

Cet onglet présente la **Taille de clé (octets)** et la **Validité (jours)** pour l'Autorité de certification (avec la **Validité de la CRL en jours** en plus pour la CA, dans la limite de 3650 jours), les certificats utilisateur, les certificats Smartcard et les certificats serveurs.

Ajouter une sous-autorité

Lorsque vous créez une sous-autorité, les écrans visibles sont similaires à ceux de la création d'une autorité racine. L'assistant de configuration pour une sous-autorité a besoin d'une référence « parente » dont il va reprendre les informations.
La CA choisie comme référence pour la sous-autorité sera la CA par défaut ou, la dernière CA sélectionnée avant d'avoir cliqué sur « **Ajouter une sous-autorité** ».

Vous devrez renseignez un CN et un identifiant dans un premier temps. Vous devez ensuite saisir le mot de passe de l'autorité parente dans la case prévue à cet effet « Mot de passe autorité parente ».
L'icône vous permet d'afficher le mot de passe en clair pour vérifier qu'il est correct.

Cliquez ensuite sur **Suivant**.

L'écran qui suit vous demande de présenter le mot de passe de votre CA et de le confirmer.
Vous pourrez également renseigner votre **E-mail**, la **Taille de clé (en octets)**, ainsi que la durée de **Validité (en jours)** de votre sous-autorité.
Vous verrez ensuite apparaître un résumé des informations saisies.

 **NOTE**

Pour visualiser votre sous-autorité au sein de la liste de gauche, déroulez l'autorité parente à laquelle celle-ci est rattachée.

Cliquez sur **Terminer**.
En cliquant sur la sous CA concernée, ses informations détaillées s'afficheront à droite de l'écran en 3 onglets :

<u>L'onglet « Détails »</u>

4 fenêtres y reprennent les données concernant, la « **Validité** » de l'autorité, son destinataire (« **Emis pour** »), son « **Emetteur** » et ses « **Empreintes** » (informations sur le produit et sa version).

<u>L'onglet « CRL »</u>

Il reprend les informations concernant la CRL : la validité incluant la dernière et la prochaine mise à jour, la grille des points de distribution et la grille de certificats révoqués, devant contenir un numéro de série, une date de révocation et un motif de révocation.

<u>L'onglet configuration</u>

Cet onglet présente la **Taille de clé (octets)** et la **Validité (jours)** pour l'Autorité de certification (avec la **Validité de la CRL en jours** en plus pour la CA, dans la limite de 3650 jours), les certificats utilisateur, les certificats Smartcard et les certificats serveurs.

Ajouter un certificat utilisateur

Dans l'assistant de configuration, l'administrateur va spécifier les informations relatives à l'utilisateur pour lequel il souhaite créer un certificat, en renseignant l'adresse e-mail de celui-ci.
Une fois le certificat généré et publié par l'administrateur, l'utilisateur recevra un mail de confirmation de création de son certificat et pourra le présenter afin de se connecter (si l'envoi d'e-mail est activé).

 **NOTE**

Le certificat utilisateur dépend, lui aussi, d'une autorité parente, il va choisir la CA par défaut.
Cliquez sur le bouton **Ajouter un certificat utilisateur**.

Nom (CN) (obligatoire)	Saisissez le nom de votre utilisateur, dans la limite de 64 caractères maximum. **NOTE** Ce champ doit être rempli afin de poursuivre la configuration.
Identifiant	Bien que le remplissage de ce champ ne soit pas obligatoire, vous pouvez ici indiquer un raccourci de votre CN, utile pour vos lignes de commande. **Exemple** Si vous aviez choisi un nom et un prénom pour votre CN, l'identifiant peut en indiquer les initiales uniquement.
E-mail (obligatoire)	Renseignez dans ce champ l'e-mail de l'utilisateur pour lequel vous souhaitez créer un certificat.

Vous devrez ensuite spécifier différentes options pour votre certificat utilisateur.

Par défaut, le champ « **Validité** » est fixé à 365 jours, et le champ **Taille de clé**, à 2048 octets.

 **NOTE**

Pour visualiser votre certificat créé au sein de la liste de gauche, déroulez l'autorité parente à laquelle celui-ci est rattaché.

Publication dans l'annuaire LDAP

Vous pouvez choisir d'associer le certificat utilisateur à votre base LDAP en cochant la case « **Publier ce certificat dans l'annuaire LDAP** ».
Si cette case est cochée, le certificat pourra être directement lié à son utilisateur si celui-ci figure dans la base LDAP et par conséquent, faciliter l'`Authentification`.
Pour cela, il faut que l'e-mail spécifié lors de la création du certificat utilisateur dans l'assistant soit identique à celui utilisé dans la fiche utilisateur de la base utilisateurs du firewall.

Mot de passe du container PKCS#12 publié (8 car. min.)	Le container PKCS#12 est un format de certificat. Il contient la clé privée et le certificat utilisateur ainsi que le certificat de l'autorité de certification. Renseignez-lui un mot de passe afin de protéger les informations des 3 éléments cités ci-dessus.
Confirmez le mot de passe	Retapez une seconde fois votre mot de passe dans ce champ afin de le confirmer.
Force du mot de passe	Ce champ indique le niveau de sécurité de votre mot de passe : « Très Faible », « Faible », « Moyen », « Bon » ou « Excellent ». Il est fortement conseillé d'utiliser les majuscules et les caractères spéciaux.

Cliquez sur **Suivant**.
Les écrans qui suivent reprennent les informations de l'autorité parente sélectionné au préalable ainsi qu'un résumé des données du certificat utilisateur.
Cliquez sur **Terminer**.
En cliquant sur le certificat concerné, ses informations détaillées s'afficheront à droite de l'écran en 1 unique onglet :

Onglet « Détails »

4 fenêtres y reprennent les données concernant, la « **Validité** » de l'autorité, son destinataire (« **Emis pour** »), son « **Emetteur** » et ses « **Empreintes** » (informations sur le produit et sa version).

Ajouter un certificat Smartcard

Le certificat Smartcard est lié à un compte *Microsoft Windows* associé à un utilisateur et un certificat. Il permet de signer et délivrer des certificats permettant l'authentification des utilisateurs enregistrés dans l'Active Directory (voir document `Configuration de l'annuaire (LDAP)\Connexion à un annuaire Microsoft Active Directory`) d'une part, mais également dans votre base LDAP.



A un utilisateur est attribué un compte Windows, par conséquent : à chaque utilisateur est attribué un certificat Smartcard. La CA utilisé doit avoir des CRLDP définis.

Nom (CN) (obligatoire)	Saisissez un nom pour le certificat Smartcard, dans la limite de 64 caractères maximum.
Identifiant	Bien que le remplissage de ce champ ne soit pas obligatoire, vous pouvez ici indiquer un raccourci de votre CN, utile pour vos lignes de commande. **Exemple** Si vous aviez choisi un nom et un prénom pour votre CN, l'identifiant peut en indiquer les initiales uniquement.
E-mail (obligatoire)	Renseignez dans ce champ l'e-mail de l'utilisateur pour lequel vous souhaitez créer un certificat.

Nom principal d'utilisateur (Windows)	Saisissez le nom de du propriétaire du compte Windows pour lequel vous souhaitez créer un certificat Smartcard.

Procédez ensuite de manière similaire à l'ajout d'un certificat utilisateur :
Spécifier les différentes options pour votre certificat Smartcard. Par défaut, le champ « **Validité** » est fixé à 365 jours, et le champ **Taille de clé**, à 1024 octets.

Vous pouvez ensuite « **Publier ce certificat dans l'annuaire LDAP** » en cochant la case correspondante, et définir un mot de passe à confirmer, pour le container PKCS#12.
Après avoir cliqué sur **Suivant**, sélectionnez une autorité parente pour votre certificat et saisissez son mot de passe. Vous verrez ensuite apparaître un résumé des données renseignées.
Cliquez sur **Terminer**.
En cliquant sur le certificat concerné, ses informations détaillées s'afficheront à droite de l'écran en 1 unique onglet :

Onglet « Détails »

4 fenêtres y reprennent les données concernant, la « **Validité** » de l'autorité, son destinataire (« **Emis pour** »), son « **Emetteur** » et ses « **Empreintes** » (informations sur le produit et sa version).

Ajouter un certificat serveur

Le certificat serveur est installé sur un serveur web et permet d'assurer le lien entre eux.
Dans le cas d'un site web, il permet de vérifier que l'URL et son DN (Nom de domaine) appartiennent bien à telle ou telle entreprise.
Définissez les propriétés du certificat serveur par le biais de l'assistant.

Nom de domaine qualifié (FQDN)	Le FQDN représente le nom complet d'un hôte dans une URL, soit un HOST (comme *www*) et un nom de domaine (de type *netasq.com*). **Exemple** *www.netasq.com*
Identifiant	Bien que le remplissage de ce champ ne soit pas obligatoire, vous pouvez ici indiquer un raccourci de votre FQDN, utile pour vos lignes de commande. **Exemple** *NETASQ* (propriétaire du FQDN)

Procédez ensuite de manière similaire à l'ajout d'un certificat utilisateur ou d'un certificat Smartcard :
Spécifier les différentes options pour votre certificat serveur. Par défaut, le champ « **Validité** » est fixé à 365 jours, et le champ **Taille de clé**, à 2048 octets.

Vous pouvez ensuite « **Publier ce certificat dans l'annuaire LDAP** » en cochant la case correspondante, et définir un mot de passe à confirmer, pour le container PKCS#12.
Après avoir cliqué sur **Suivant**, sélectionnez une autorité parente pour votre certificat et saisissez son mot de passe. Vous verrez ensuite apparaître un résumé des données renseignées.
Cliquez sur **Terminer**.

En cliquant sur le certificat concerné, ses informations détaillées s'afficheront à droite de l'écran en 1 unique onglet :

Onglet « Détails »

4 fenêtres y reprennent les données concernant, la « **Validité** » de l'autorité, son destinataire (« **Emis pour** »), son « **Emetteur** » et ses « **Empreintes** » (informations sur le produit et sa version).

Importer un fichier

En cliquant sur ce bouton, vous importerait un fichier (contenant votre certificat) par le biais de l'assistant de configuration.
Cela évite de passer par les étapes de création de CA, de sous CA ou certificats.

Fichier à importer

En cliquant sur l'icône ..., à droite du champ, vous pourrez parcourir votre ordinateur ou votre navigateur web à la recherche d'un certificat (si vous en avez créé au préalable).

Format du fichier

3 formats de fichier sont proposés :

- **Format base 64** (**PEM** - *Privacy Enhanced Mail*), Il permet l'encodage des certificats X509 en base 64. Un certificat de type PEM se présente de la manière suivante :

-----BEGIN CERTIFICATE-----
MIIDdzCCAuCgAwIBAgIBBzANBgkqhkiG9w0BAQQFADCBpDELMAkGA1UEBhMCQ0gxCzAJBgNVBAgTAkdFM
Q8wDQYD
VQQHEwZHZW5ldmExHTAbBgNVBAoTFFVuaXZlcnNpdHkgb2YgR2VuZXZhMSQwIgYDVQQLExtVTklHRSBDZ
XJ0aWZpY
2F0ZSBBdXRob3JpdHkxETAPBgNVBAMTCFVuaUdlIENBMR8wHQYJKoZIhvcNAQkBFhB1bmlnZWNhQHVuaW
dlLmNoMB
4XDTk5MTAwNDE2MjI1N1oXDTAwMTAwMzE2MjI1N1owgbExCzAJBgNVBAYTAkNIMQswCQYDVQQIEwJHRT
EPMA0GA1
UEBxMGR2VuZXZhMR0wGwYDVQQKExRVbml2ZXJzaXR5IG9mIEdlbmV2YTEeMBwGA1UECxMVRGl2aXNpb
24gSW5mb
3JtYXRpcXVlMRowGAYDVQQDExFBbGFpbiBIdWdlbnRvYmxlcjEpMCcGCSqGSIb3DQEJARYaQWxhaW4uSHV
nZW50b2J
sZXJAdW5pZ2UuY2gwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALIL5oX/FR9ioQHM0aXxfDELkhPKkw
8jc6I7BtSY
Jk4sfqvQYqvOMt1uugQGkyIuGhP2djLj6Ju4+KyKKQVvDJIu/R1zFX1kkqOPt/A2pCLkisuH7nDsMbWbep0hDTVN
ELoKVoVIA
azwWMFlno2JuHJgUcs5hWskg/azqI4d9zy5AgMBAAGjgakwgaYwJQYDVR0RBB4wHIEaQWxhaW4uSHVnZW50
b2JsZXJAd
W5pZ2UuY2gwDAYDVR0T200BAUwAwIBADBcBglghkgBhvhCAQ0ETxZNVU5JR0VDQSBjbGllbnQgY2VydGlma
WNhdGUsI
HNlZSBodHRwOi8vdW5pZ2VjYS51bmlnZS5jaCBmb3IgbW9yZSBpbmZvcm1hdGlvbnMwEQYJYIZIAYb4QgEBB
AQDAgSwM
A0GCSqGSIb3DQEBBAUAA4GBACQ9Eo67A3UUa6QBBNJYbGhC7zSjXiWySvj6k4az2UqTOCT9mCNnmPR5I3
Kxr1GpWT
oH68LvA30inskP9rkZAksPyaZzjT7aL//phV3ViJfreGbVs5tiT/cmigwFLeUWFRvNyT9VUPUov9hGVbCc9x+v05uY7t
3UMeZejj8
zHHM+
-----END CERTIFICATE----

Les balises "-----BEGIN CERTIFICATE-----" et "-----END CERTIFICATE-----" encadrent le bloc de "n" lignes de chacune 64 caractères de type [A-Za-z0-9/+].

C'est un format qui transite souvent par e-mail car celui-ci résiste très bien aux déformations des logiciels de messagerie.

Le fichier PEM est un fichier texte contenant ce type d'information.

De même le fichier CRL contient des chaînes de caractères codées en base 64 encadrées par des balises

du type : "-----BEGIN X509 CRL-----" et "-----END X509 CRL-----".

Le fichier de clé privée, quant à lui, contient des chaînes de caractères codées en base 64 encadrées par

des balises du type : "-----BEGIN RSA PRIVATE KEY-----" et "-----END RSA PRIVATE KEY-----".

	Format binaire (**DER** - *Distinguished Encoding Rules),* celui-ci contient le certificat de l'utilisateur en format binaire. **Container** (**PKCS#12**), il contient la clé privée et le certificat utilisateur ainsi que le certificat de l'autorité de certification. De plus, celui-ci est crypté.
Mot de passe du fichier (si PKCS#12)	Définissez un mot de mot de passe pour le fichier PKCS#12, si c'est ce format pour lequel vous avez opté (le même que pour la Publication du certificat utilisateur dans le LDAP. L'icône vous permet d'afficher le mot de passe en clair pour vérifier qu'il est correct.
Eléments du fichier à importer	Etant donné que chaque format de fichier contient des éléments différents, vous pouvez choisir d'importer tout ou une partie de votre fichier via les choix suivants. **Tous** : Importez tous les éléments contenus dans vos fichiers. Ou choisissez de ne garder que ceux-ci : **Certificat(s)** **Clé(s) privée(s)** **CRL** **Autorité de Certification (CA)** **Requête(s)**
Ecraser le contenu existant dans la PKI	Si vous cochez cette case, les contenus similaires aux éléments ci-dessus seront écrasés dans la PKI, en faveur des nouveaux certificats/clés privées/CA et requêtes.

Cliquez sur **Suivant**. Vous verrez s'afficher un résumé des données l'importation de votre fichier (son nom, son format et les éléments à importer).
Cliquer sur **Terminer**.

Supprimer

Ce bouton est lié à la colonne de gauche. Sélectionnez dans la liste la CA, sous CA ou le certificat que vous souhaitez retirer, et cliquez sur **Supprimer**.

Téléchargement

Ce bouton vous permet de télécharger les CA, sous CA et les certificats, en les sélectionnant dans la liste de gauche.

1) Une fenêtre d'ouverture s'affichera en vous proposant les options :

« **Ouvrir avec – Parcourir** » ou « **Enregistrer le fichier** »

Un assistant d'importation de certificat apparaît ensuite, si vous avez sélectionné « Ouvrir avec ». Il aide à copier des certificats, des listes de certificats de confiance et des CRL depuis votre disque dur vers un magasin de certificats.

Un certificat, émis par une autorité de certification est une confirmation de votre identité et contient des informations utilisées pour protéger vos données ou établir des connexions réseau sécurisées.

2) Cliquez sur **Suivant** et choisissez le fichier à importer.

3) Entrez ensuite le mot de passe. Deux cases à cocher vous sont proposées :

- Activer la protection renforcée des clés privées. La clé privée vous sera demandée chaque fois qu'elle est utilisée par une application si vous activez cette option.
- Marquer cette clé comme exportable. Cela vous permettra de sauvegarder de transporter vos clés ultérieurement.

4) Cliquez sur **Suivant**, vous accédez au « magasin de certificats ». Windows peut sélectionner automatiquement le magasin de certificats, ou vous pouvez spécifier l'emplacement du certificat.

Deux options vous sont proposées :

- Sélectionner automatiquement le magasin de certificats selon le type de certificat
- Placer tous les certificats dans le magasin suivant : choisissez l'emplacement en cliquant sur **« Parcourir »**.

5) Cliquez sur **Suivant**, la page de fin de l'Assistant Importation de certificat s'affiche et résume les paramètres que vous avez configurés

6) Cliquez sur **Terminer**. Il est possible qu'un écran « Avertissement de Sécurité » apparaisse et vous demande de confirmer l'installation de votre certificat (ce facteur varie selon la configuration de votre Windows, ou de votre OS).


NOTE

Tout problème rencontré au sein de cette procédure n'est pas du ressort de NETASQ.

Publication LDAP

Ce bouton vous permet de publier dans l'annuaire LDAP une CA, sous CA ou un certificat en le sélectionnant dans la liste de gauche.

Créer CRL

Ce bouton permet de créer une CRL pour une CA, sous CA ou certificat apparaissant dans la liste de gauche.
Vous devrez entrer le mot de passe protégeant l'autorité, puis cliquez sur **Créer CRL**.
Lorsque vous voudrez vérifier qu'une CRL est bien à jour, tapez la commande « checkcrl –d ».
Pour qu'une CRL soit correctement entrée, n'oubliez pas d'indiquer le « http// » + le FQDN complet + /ca.crl


NOTE

» Cette icône en haut à droite de l'écran vous propose soit, de définir l'une des CA comme autorité « par défaut » par le biais d'une fenêtre de confirmation : pour cela positionnez-vous sur la CA voulue et sélectionnez « par défaut ». Vous pouvez également « Vérifier l'utilisation » de votre CA.

Si celle-ci est déjà utilisée dans un module, vous la verrez apparaître au sein de l'arborescence des modules de gauche.

CONFIGURATION

L'écran de configuration – administration se compose de 3 onglets :

- `Configuration générale` : définition des caractéristiques du firewall (nom, langue, clavier) des paramètres de date et d'heure, ainsi que des serveurs NTP.
- `Administration du Firewall` : configuration des accès à l'interface d'administration du firewall (port d'écoute, SSH etc.)
- `Paramètres réseaux` : configuration du serveur proxy, des limites VLAN et de la résolution DNS.

L'onglet « Configuration générale »

L'onglet `Configuration générale` permet la modification des paramètres suivants :

Configuration générale

Nom du firewall	Ce nom est utilisé dans les mails d'alarmes envoyés à l'administrateur et est affiché sur la fenêtre principale du firewall. Ce nom peut-être quelconque.
Langue du Firewall (traces)	Choix de la langue du boitier, limité à **Français** et **Anglais**. Ceci est utilisé pour les traces de types log, syslog et la configuration CLI.
Clavier (console)	Type de clavier supporté par le firewall. 5 langues sont disponibles : **Anglais, Français, Italien, Polonais, Suisse**.

Configuration du temps

Date	Date du firewall. Choisissez la date sur le calendrier. Ce champ est grisé si la configuration NTP est activée.
Heure	Heure du firewall. Ce champ est grisé si la configuration NTP est activée.
Synchroniser avec votre machine	En cliquant sur ce bouton, le firewall se mettra à l'heure de votre machine. Ce champ est grisé si la configuration NTP est activée.
Fuseau horaire	Fuseau horaire défini pour le firewall (GMT par défaut). **AVERTISSEMENT** Un changement de fuseau horaire entraîne un redémarrage du firewall.
Maintenir le firewall à l'heure (NTP)	Le Protocole d'Heure Réseau (*Network Time Protocol* ou NTP) est un protocole qui permet de synchroniser l'horloge locale de vos machines sur une référence d'heure via votre réseau. En cochant cette option, votre firewall sera automatiquement synchronisé à l'heure locale.

 **REMARQUE**
La date et l'heure auxquelles votre firewall NETASQ est réglé sont importantes : elles vous permettent de situer dans le temps un événement enregistré dans les fichiers de log. Elles servent également à la programmation horaire des configurations.

Liste des serveurs NTP

Ce tableau n'est accessible que si vous avez coché l'option **Maintenir le firewall à l'heure (NTP)**. Si vous n'avez pas effectué cette manipulation au préalable, la liste des serveurs NTP sera grisée.

Serveurs NTP (machine ou groupe-plages d'adresses) (15 max)	Le serveur NTP représente l'horloge distante sur laquelle on va choisir de synchroniser son firewall. Vous pouvez en **Ajouter** ou en **Supprimer** en cliquant sur les boutons correspondants. Lorsque vous cliquez sur **Ajouter**, une ligne vierge vient s'ajouter à la liste des serveurs NTP. Vous pouvez choisir un objet au sein de la liste déroulante ou en créer un en cliquant sur cette icône . Il sera ainsi possible de créer une machine, une plage d'adresses IP ou un groupe. Cliquez sur **Appliquer** une fois les données du nouvel objet renseignées.
Mot de passe (ASCII)	Bien que cela soit optionnel, vous pouvez renseigner un mot de passe pour votre serveur NTP, avec lequel vous pourrez vous authentifier.

L'onglet « Administration du Firewall »

Accès à l'interface d'administration du Firewall

Autoriser le compte 'admin' à se connecter	Le compte 'admin' est le seul compte ayant tous les droits. Il peut se connecter sans certificat et par là-même, forcer une connexion. Il est nécessaire de cocher cette case si vous souhaitez conserver ces accès privilégiés. **AVERTISSEMENT** Ce compte est à considérer comme « dangereux », aux vues de l'étendue des possibilités de configuration et des accès lui étant attribués.
Port d'écoute	Ce champ représente le port sur lequel vous pourrez accéder à l'interface d'administration (https, tcp/443 par défaut).  **NOTE** Vous pouvez créer un port d'écoute supplémentaire en cliquant sur l'icône . **AVERTISSEMENT** L'objet ne peut être que de type « TCP » (et non « UDP »).
Activer la protection contre les attaques par force brute	Les attaques par force brute se définissent par des tentatives de connexion répétées au firewall, en testant toutes les combinaisons de mot de passe possibles.

	En cochant cette case, vous empêcherez cela et dégriserez les deux champs suivants, afin de limiter les tentatives de connexion.
Tentatives d'authentification autorisées	Nombre d'authentification possibles en cas d'échec de connexion (erreur d'identifiant ou de mot de passe/sensibilité à la casse par exemple). Les tentatives d'authentification autorisées sont limitées à 3 par défaut.
Durée de blocage (minutes)	Temps durant lequel vous ne pourrez pas vous authentifier après le nombre d'échecs spécifié ci-dessus, ni durant lequel vous pourrez vous connecter. La durée de blocage ne peut excéder 60 minutes.

Accès aux pages d'administration du Firewall

Ajouter un serveur	Choisissez un serveur au sein de la liste déroulante d'objets proposés. Celui-ci sera considéré comme un **Poste d'administration autorisé** à se connecter à l'interface d'administration. Cela peut être une machine, un groupe de machines, un réseau ou une plage d'adresses.
Supprimer	Sélectionner la ligne à retirer de la liste et cliquez sur **Supprimer**.

Accès distant par SSH

Activer l'accès par SSH	Le SSH (*Secure Shell*) est un protocole qui permet de se connecter à une machine distante avec une liaison sécurisée. Les données sont chiffrées entre machines. Le SSH permet également d'exécuter des commandes sur un serveur distant. Cochez cette case si vous souhaitez vous connecter à distance en mode console, et ce, de manière totalement sécurisée. **NOTE** En cochant cette option, vous dégriserez les deux champs du dessous.
Autoriser l'utilisation de mot de passe	Le mot de passe en question correspond à celui du compte « admin », étant le seul à pouvoir se connecter en SSH. L'« admin » devra le présenter pour accéder au firewall via une machine distante. Vous pouvez aussi utiliser un couple clé privée/clé publique pour vous authentifier.
Port d'écoute	Ce champ représente le port sur lequel vous pourrez accéder à l'interface d'administration (https, tcp/443 par défaut). **NOTE** Vous pouvez créer un port d'écoute supplémentaire en cliquant sur l'icône +. **AVERTISSEMENT** L'objet ne peut être que de type « TCP » (et non « UDP »).

L'onglet « Paramètres réseaux »

Serveur proxy

Le Firewall utilise un proxy pour accéder à Internet	Cochez cette case afin de dégriser les champs du dessous et permettre au firewall d'utiliser un proxy pour accéder à Internet de manière sécurisée. Ceci est utilisé par ActiveUpdate et LicenceUpdate.
Serveur	Ce champ permet de spécifier l'objet correspondant au serveur utilisé par le firewall comme proxy.
Port	Ce champ permet de spécifier le port utilisé par le firewall pour contacter le proxy.
Identifiant	Ce champ permet de définir un identifiant utilisé par le firewall pour s'authentifier auprès du proxy.
Mot de passe	Définissez un mot de passe que vous devrez fournir pour accéder au serveur proxy.

Limites

VLAN disponibles (max 128)	Limitation du nombre de VLAN disponibles dans la configuration réseau. Le nombre de VLAN disponibles par défaut est 64, changez ce nombre provoque un reboot de votre boîtier.

Résolution DNS

Liste des serveurs DNS utilisés par le firewall

Les serveurs DNS permettent au firewall de résoudre (connaître son adresse IP à partir d'un nom de machine) les objets ou machines configurés en Résolution DNS « Automatique ».

Ajouter	Lorsque vous cliquez sur ce bouton, une ligne vierge vient s'ajouter au tableau et vous permet de sélectionner un serveur DNS au sein de la liste déroulante.
Supprimer	Sélectionnez la ligne à retirer du tableau et cliquez sur **Supprimer**.
Monter	Placer la ligne sélectionnée au dessus de la ligne précédente.
Descendre	Placer la ligne sélectionnée au dessous de la ligne suivante.

CONFIGURATION DE L'ANNUAIRE (LDAP)

LDAP est un protocole standard permettant de gérer des annuaires, c'est-à-dire d'accéder à des bases d'informations sur les utilisateurs d'un réseau par l'intermédiaire de protocoles TCP/IP.

Les firewalls NETASQ embarquent une base LDAP interne. Celle-ci stocke les informations relatives aux utilisateurs devant s'authentifier pour passer au travers du firewall. Il est toutefois possible de connecter le firewall à une base LDAP externe qui se trouve sur une machine distante.

Le module de Configuration de l'annuaire (accessible dans le menu `Utilisateurs\Configuration de l'annuaire`) comporte un assistant de configuration en première page, vous proposant de choisir votre annuaire et de l'initialiser.

- Connexion à un annuaire Microsoft Active Directory
- Connexion à un annuaire LDAP externe
- Création d'un LDAP interne

En fonction de votre choix, l'étape suivante est variable, la configuration d'un LDAP externe réclamant plus de renseignements.

Chacune des configurations de ces annuaires comporte 3 étapes, sélectionnez la base LDAP choisie en cochant la case correspondante.

Création d'un LDAP interne

Ce type d'annuaire est hébergé par votre firewall multifonctions NETASQ, vos informations y seront stockées une fois l'annuaire LDAP construit.

Etape 1 : Choix de l'annuaire

Comme précisé ci-dessus, il faut cocher la base LDAP choisie pour valider votre choix. Ceci est la première étape de la configuration d'un annuaire.
Cochez la case **Création d'un LDAP interne** et cliquez sur **Suivant**.

Etape 2 : Accès à l'annuaire

Lors de cette seconde étape, vous devez renseigner les informations générales concernant la base LDAP que vous désirez créer. Les informations saisies se retrouveront dans le schéma de l'annuaire LDAP de votre firewall.

Organisation	Le nom de votre société (ex : NETASQ).
Domaine	Le pays dans lequel se trouve votre société (ex : fr).
Mot de passe	Définition du mot de passe NetasqAdmin.
Confirmer	Confirmation du mot de passe d'administration LDAP, que vous venez de renseigner dans le champ précédent.
Force du mot de passe	Ce champ indique le niveau de sécurité de votre mot de passe : « Très Faible », « Faible », « Moyen », « Bon » ou « Excellent ». Il est fortement conseillé d'utiliser les majuscules et les caractères spéciaux.

 **NOTE**

Seul le mot de passe sera modifiable par la suite, une fois que vous aurez configuré votre LDAP interne.

Cliquez sur **Suivant** pour passer à l'étape 3.

Etape 3 : Authentification

Votre annuaire interne étant désormais défini, cet écran vous permet d'autoriser l'accès à la base LDAP et d'activer des options relatives à l'authentification. Il propose 3 services :

Autoriser l'accès à la base LDAP	Cette option permet de rendre l'annuaire LDAP public.
Autoriser l'accès au portail captif depuis les réseaux protégés (interfaces internes)	Restreinte aux interfaces internes, en cochant cette option, vous activez l'authentification sur le portail captif. Ceci équivaut à l'option **Activer le portail captif** « depuis les interfaces internes » du module `Authentification` (dans le menu `Utilisateurs\Authentification`).
Activer l'enrôlement des utilisateurs via le portail web	En activant cette option, tout utilisateur dépourvu d'un compte pour s'authentifier sur le firewall, peut remplir un formulaire de demande d'enrôlement sur le portail captif. **NOTE** La requête d'enrôlement devra être avalisée par l'administrateur pour que le compte soit effectif. Votre requête pourra être validée ou refusée par un administrateur.

Cliquez sur **Terminer**.

Ecran de l'annuaire LDAP interne

Une fois que la configuration de l'annuaire LDAP effectuée, vous accédez à l'écran du LDAP interne qui présente les éléments suivants :

Activer l'utilisation de l'annuaire utilisateur	Cette option permet de démarrer le service LDAP. Si la case n'est pas cochée, le module est inactif.

Annuaire LDAP interne

Organisation	Ce champ reprend le nom de votre société, renseigné au préalable.
Domaine	Ce champ reprend le domaine de votre société.
Identifiant	Le login qui vous permet de vous connecter à la base LDAP interne.
Mot de passe	Le mot de passe permettant au firewall de se connecter à l'annuaire. Il est possible de le modifier.
Confirmation	Confirmation du mot de passe d'administration LDAP, que vous venez de renseigner dans le champ précédent.
Force du mot de passe	Ce champ indique le niveau de sécurité de votre mot de passe : « Très Faible », « Faible », « Moyen », « Bon » ou « Excellent ». Il est fortement conseillé d'utiliser les majuscules et les caractères spéciaux.

Accès au LDAP interne

Activer l'accès non chiffré (PLAIN)	Les données saisies ne seront pas chiffrées, mais affichées en clair.
Activer l'accès SSL. (Certificat SSL présenté par le serveur)	Afin de mettre en place l'accès SSL, vous devrez sélectionner un certificat serveur préalablement généré par votre autorité racine, ou un certificat importé.

Configuration avancée

Fonction de hachage des mots de passe : La méthode de chiffrement des mots de passe des nouveaux utilisateurs.

Certaines méthodes d'authentification (comme LDAP) doivent stocker le mot de passe utilisateur sous la forme d'un hash (résultat d'une fonction de hachage appliquée au mot de passe) qui évite le stockage en clair de ce mot de passe.

Vous devez choisir la méthode de hash désirée parmi :

SHA	« Secure Hash Algorithm ». Cette méthode de chiffrement permet d'établir une chaîne de caractères de 160 bits ou octets (appelé « clé ») qui sert de référence pour l'identification.
MD5	« Message Digest ». Cet algorithme permet de vérifier l'intégrité des données saisies, en générant une « clé MD5 », de 128 bits. **REMARQUE** Cette méthode possédant un nombre d'octets moins élevé, et par conséquent, un niveau de sécurité plus faible, celle-ci est moins robuste aux attaques.
SSHA	« Salt Secure Hash Algorithm ». Repose sur le même principe que SHA, mais contient en plus une fonction de « salage » de mot de passe, qui consiste à ajouter une séquence de bit aux données saisies, afin de les rendre encore moins lisibles. **NOTE** Cette variante de SHA utilise une valeur aléatoire pour diversifier l'empreinte du mot de passe. Deux mots de passe identiques auront ainsi deux empreintes différentes. Cette méthode de chiffrement est la plus sécurisée et son utilisation est fortement recommandée.
SMD5	« Salt Message Digest ». Repose sur le même principe que MD5, avec la fonction de salage de mot de passe en plus.
CRYPT	Le mot de passe est protégé par l'algorithme CRYPT, dérivé de l'algorithme DES permettant le chiffrement par bloc, en utilisant des clés de 56 bits. Il est peu conseillé, possédant un niveau de sécurité relativement faible.
Aucune	Pas de chiffrement du mot de passe, celui-ci est stocké en clair. **AVERTISSEMENT** Cette méthode est très peu recommandée car vos données ne sont pas protégées.

Lorsque vous avez terminé votre configuration, vous pouvez cliquer sur **Appliquer** pour l'activer.



NOTE

Pour se connecter à un autre annuaire et revenir à l'assistant de configuration à tout moment, cliquez sur la baguette magique ( ) en haut de l'écran à droite.

AVERTISSEMENT

Sélectionner l'icône entraine une réinitialisation de la base LDAP et de ce fait, la suppression définitive de la précédente configuration de l'annuaire et de ses constituants.

Connexion à un annuaire LDAP externe

Le LDAP externe est un annuaire auquel votre firewall multifonctions NETASQ va se connecter.

Etape 1 : Choix de l'annuaire

Sélectionnez la base LDAP correspondant à votre choix. Ceci est la première étape de la configuration de cet annuaire.
Cochez la case **Connexion à un annuaire LDAP externe** et cliquez sur **Suivant**.

Etape 2 : Accès à l'annuaire

Serveur	Vous devez choisir un objet correspondant à votre serveur LDAP au sein de la liste déroulante. Cet objet doit être créé au préalable et référencer l'adresse IP de votre serveur LDAP.
Port	Vous devez renseigner le port d'écoute de votre serveur LDAP. Le port par défaut est : 389.
Domaine racine (Base DN)	Vous devez renseigner le Domaine racine (DN) de votre annuaire. Le DN représente le nom d'une entrée, sous la forme d'un chemin d'accès à celle-ci, depuis le sommet de l'arborescence. **Exemple de DN** o=NETASQ,dc=COM
Identifiant	Un compte administrateur permettant au firewall de se connecter sur votre serveur LDAP et d'effectuer des modifications (droits en lecture et écriture) sur certains champs. Nous vous recommandons de créer un compte spécifique pour le firewall et de lui attribuer les droits uniquement sur les champs qui lui sont nécessaires. **Exemple** cn=identifiant.
Mot de passe	Le mot de passe associé à l'identifiant pour vous connecter sur le serveur LDAP. **NOTE** L'icône « clé » () permet d'afficher le mot de passe en clair pour vérifier qu'il n'est pas erroné.

Cliquez sur **Suivant** pour passer à l'étape 3.

Etape 3 : Authentification

Autoriser l'accès au portail captif depuis les réseaux protégés (interfaces internes)	Restreinte aux interfaces internes, en cochant cette option, vous activez l'authentification sur le portail captif. Ceci équivaut à l'option **Activer le portail captif** « depuis les interfaces internes » du module `Authentification` (dans le menu `Utilisateurs\Authentification`).

 **NOTE**

Lors de la création d'un nouvel utilisateur, la méthode de hachage SHA sera utilisée pour le stockage des mots de passe, par défaut.

Ecran de l'annuaire LDAP externe

Une fois que la configuration de l'annuaire LDAP effectuée, vous accédez au LDAP externe qui présente les éléments suivants :

Onglet « Annuaire externe »

La page affichée présente une fenêtre récapitulative des informations saisies pour votre LDAP externe et différents services concernant l'accès à votre annuaire.

Activer l'utilisation de l'annuaire utilisateur	Cette option permet de démarrer le service LDAP. Si la case n'est pas cochée, le module est inactif.

Annuaire distant

Serveur	Ce champ reprend le nom du serveur que vous avez préalablement rempli à la page précédente.
Port	Ce champ reprend le port d'écoute que vous avez préalablement sélectionné à la page précédente.
Domaine racine (Base DN)	Le Domaine racine de votre annuaire.
Identifiant	L'identifiant permettant au firewall de se connecter sur votre serveur LDAP.
Mot de passe	Le mot de passe créé sur le firewall pour vous connecter sur le serveur LDAP.

Connexion sécurisée (SSL)

Activer l'accès en SSL	Cette option permet d'effectuer une vérification de votre certificat numérique généré par l'autorité racine du firewall. Les informations sont chiffrées en SSL. Cette méthode utilise le port 636. L'accès public au LDAP est protégé avec le protocole SSL. **NOTE** Si cette option n'est pas cochée, l'accès est non chiffré.
Vérifier que le nom du serveur correspond au FQDN présenté dans le certificat SSL	Le FQDN représente le nom complet d'un hôte dans une URL, soit un HOST (comme *www*) et un nom de domaine (de type *netasq.com*) **Exemple** *www.netasq.com* Si cette case est cochée, la vérification du certificat du serveur est activée. Le certificat SSL contient un FQDN, avec lequel le nom du serveur doit correspondre pour que les données soient correctement protégées.
Autorité de certification	Cette option permet de sélectionner l'autorité de certification qui sera comparée au certificat serveur délivré par le serveur LDAP, afin d'assurer l'authenticité de la connexion au serveur LDAP. Vous pouvez cliquer sur l'icône « loupe » ( ) pour effectuer une recherche de la CA correspondante. **NOTE** Cette case sera grisée par défaut si l'option précédente **Vérifier que le nom du serveur correspond au FQDN présenté dans le certificat SSL** n'est pas cochée.

Configuration avancée

Serveur de rechange	Ce champ permet de définir un serveur de remplacement au cas où le serveur principal tomberait. Vous pouvez le sélectionner parmi la liste d'objets proposés dans la liste déroulante. En cliquant sur le bouton **Tester l'accès à l'annuaire** au dessous, une fenêtre vous précisera si votre serveur principal est opérationnel. Vous pourrez cliquez sur **OK.**

Cliquez sur **Appliquer** pour valider votre configuration.

Onglet « Structure»

Accès en lecture

Filtre de sélection des utilisateurs	Lors de l'utilisation du firewall en interaction avec une base externe, seuls les utilisateurs correspondants au filtre seront utilisés. Par défaut ce filtre correspond à *ObjectClass = InetOrgPerson*.
Filtre de sélection des groupes d'utilisateurs	Lors de l'utilisation du firewall en interaction avec une base externe, seuls les Groupes d'utilisateurs correspondants au filtre seront utilisés. Par défaut ce filtre correspond à *ObjectClass = GroupOfNames*.
Branche de l'autorité de certification	Ce champ définit l'emplacement de l'autorité de certification présente dans la base LDAP externe. Cet emplacement est notamment utilisé lors de la recherche de la CA utilisé pour la méthode d'authentification SSL. **NOTE** Il n'est pas indispensable de configurer ce champ mais dans ce cas, pour que la méthode d'authentification SSL fonctionne, il faut spécifier la CA dans la liste des CA de confiance dans la configuration de la méthode SSL. (Voir menu `Utilisateurs`\module `Authentification`\onglet `Méthodes disponibles` : il faut ajouter la méthode d'authentification **Certificat (SSL)** et indiquer la CA dans la colonne de droite « Autorités de confiance (C.A) »)

Correspondance d'attributs

Appliquer un modèle : Ce bouton vous propose de choisir parmi 3 serveurs LDAP, celui que vous appliquerez pour définir vos attributs :

- OpenLDAP : serveur LDAP.
- Microsoft Active Directory (AD) : services d'annuaires LDAP pour les systèmes d'exploitation sous Windows.
- Open Directory : répertoire de sites web sous licence *Open Directory*

Attributs de l'annuaire	Cette colonne représente la valeur donnée à l'attribut au sein de l'annuaire externe. **Exemples :** *Cn= NETASQ* *telephoneNumber= +33 (0)3 61 96 30* *mail = salesadmin@netasq.com*

L'annuaire est en lecture seule. La création d'utilisateurs et de groupes ne sera pas autorisée : Si cette case est cochée, vous ne pourrez effectuer aucune action d'écriture.

Accès en écriture

Branche 'utilisateurs'	Donnez le nom de la branche LDAP pour stocker les utilisateurs. **Exemple** ou=users.
Branche 'groupes'	Donnez le nom de la branche LDAP pour stocker les groupes d'utilisateurs. **Exemple** ou=groups.

Configuration avancée

Caractères protégés	Pour certains serveurs externes, il est nécessaire d'ajouter un \ pour que les requêtes LDAP soient comprises

Hachage des mots de passe : La méthode de chiffrement des mots de passe des nouveaux utilisateurs.

Certaines méthodes d'authentification (comme LDAP) doivent stocker le mot de passe utilisateur sous la forme d'un hash (résultat d'une fonction de hachage appliquée au mot de passe) qui évite le stockage en clair de ce mot de passe.

Vous devez choisir la méthode de hash désirée parmi :

SHA	« Secure Hash Algorithm ». Cette méthode de chiffrement permet d'établir une chaîne de caractères de 160 bits ou octets (appelé « clé ») qui sert de référence pour l'identification.
MD5	« Message Digest ». Cet algorithme permet de vérifier l'intégrité des données saisies, en générant une « clé MD5 », de 128 bits. **REMARQUE** Cette méthode possédant un nombre d'octets moins élevé, et par conséquent, un niveau de sécurité plus faible, celle-ci est moins robuste aux attaques.
SSHA	« Salt Secure Hash Algorithm ». Repose sur le même principe que SHA, mais contient en plus une fonction de « salage » de mot de passe, qui consiste à ajouter une séquence de bit aux données saisies, afin de les rendre encore moins lisibles. **NOTE** Cette variante de SHA utilise une valeur aléatoire pour diversifier l'empreinte du mot de passe. Deux mots de passe identiques auront ainsi deux empreintes différentes. Cette méthode de chiffrement est la plus sécurisée et son utilisation est fortement recommandée.
SMD5	« Salt Message Digest ». Repose sur le même principe que MD5, avec la fonction de salage de mot de passe en plus.
CRYPT	Le mot de passe est protégé par l'algorithme CRYPT, dérivé de l'algorithme DES permettant le chiffrement par bloc, en utilisant des clés de 56 bits. Il est peu conseillé, possédant un niveau de sécurité relativement faible.
Aucune	Pas de chiffrement du mot de passe, celui-ci est stocké en clair. **AVERTISSEMENT** Cette méthode est très peu recommandée car vos données ne sont pas protégées.

Une fois votre algorithme sélectionné, vous pouvez cliquer sur **Appliquer** pour valider votre configuration.

Connexion à un annuaire Microsoft Active Directory

A l'instar des annuaires interne et externe, l'Active Directory propose les mêmes fonctionnalités de gestion des utilisateurs développées par Microsoft, et utilisant le système d'exploitation *Windows*.

Etape 1 : Choix de l'annuaire

Sélectionnez l'annuaire correspondant à votre choix. Ceci est la première étape de la configuration de cet annuaire.
Cochez la case **Connexion à un annuaire Microsoft Active Directory** et cliquez sur **Suivant**.

Etape 2 : Accès à l'annuaire

Serveur	Vous devez choisir un objet correspondant à votre serveur LDAP au sein de la liste déroulante. Cet objet doit être créé au préalable et référencer l'adresse IP de votre serveur LDAP.
Port	Vous devez renseigner le port d'écoute de votre serveur LDAP. Le port par défaut est : 389.
Domaine racine (Base DN)	Vous devez renseigner le Domaine racine (DN) de votre annuaire. Le DN représente le nom d'une entrée, sous la forme d'un chemin d'accès à celle-ci, depuis le sommet de l'arborescence. **Exemple de DN** o=NETASQ,dc=COM
Identifiant	Un compte administrateur permettant au firewall de se connecter sur votre serveur LDAP et d'effectuer des modifications (droits en lecture et écriture) sur certains champs. Nous vous recommandons de créer un compte spécifique pour le firewall et de lui attribuer les droits uniquement sur les champs qui lui sont nécessaires. **Exemple** cn=identifiant.
Mot de passe	Le mot de passe associé à l'identifiant pour vous connecter sur le serveur LDAP. **NOTE** L'icône « clé » ( ) permet d'afficher le mot de passe en clair pour vérifier qu'il n'est pas erroné.

Cliquez sur **Suivant** pour passer à l'étape 3.

Etape 3 : Authentification

Autoriser l'accès au portail captif depuis les réseaux protégés (interfaces internes)	Restreinte aux interfaces internes, en cochant cette option, vous activez l'authentification sur le portail captif. Ceci équivaut à l'option Activer le portail captif « depuis les interfaces internes» du module `Authentification` (dans le menu `Utilisateurs\Authentification`).



NOTE
Lors de la création d'un nouvel utilisateur, la méthode de hachage SHA sera utilisée pour le stockage des mots de passe.

Ecran de l'annuaire Microsoft Active Directory

ONGLET « ANNUAIRE ACTIVE DIRECTORY »

Une fois que la configuration de l'annuaire effectuée, vous accédez à l'Active Directory qui présente les éléments suivants :

Activer l'utilisation de l'annuaire utilisateur	Cette option permet de démarrer le service LDAP. Si la case n'est pas cochée, le module est inactif.

Annuaire distant

Serveur	Ce champ reprend le nom du serveur que vous avez préalablement rempli à la page précédente.
Port	Ce champ reprend le port d'écoute que vous avez préalablement sélectionné à la page précédente.
Domaine racine (Base DN)	Le Domaine racine de votre annuaire.
Identifiant	L'identifiant permettant au firewall de se connecter sur votre serveur LDAP.
Mot de passe	Le mot de passe créé sur le firewall pour vous connecter sur le serveur LDAP.

Connexion sécurisée (SSL)

Activer l'accès en SSL	Cette option permet d'effectuer une vérification de votre certificat numérique généré par l'autorité racine du firewall. Les informations sont chiffrées en SSL. Cette méthode utilise le port 636. L'accès public au LDAP est protégé avec le protocole SSL. **NOTE** Si cette option n'est pas cochée, l'accès est non chiffré.
Vérifier que le nom du serveur correspond au FQDN présenté dans le certificat SSL	Le FQDN représente le nom complet d'un hôte dans une URL, soit un HOST (comme *www*) et un nom de domaine (de type *netasq.com*) **Exemple** *www.netasq.com* Si cette case est cochée, la vérification du certificat du serveur est activée. Le certificat SSL contient un FQDN, avec lequel le nom du serveur doit correspondre pour que les données soient correctement protégées.
Autorité de certification	Cette option permet de sélectionner l'autorité de certification qui sera comparée au certificat serveur délivré par le serveur LDAP, afin d'assurer l'authenticité de la connexion au serveur LDAP. Vous pouvez cliquer sur l'icône « loupe » ( ) pour effectuer une recherche de la CA correspondante. **NOTE** Cette case sera grisée par défaut si les deux options ci-dessus ne sont pas cochées.

Configuration avancée

Serveur de rechange	Ce champ permet de définir un serveur de remplacement au cas où le serveur principal tomberait. Vous pouvez le sélectionner parmi la liste d'objets proposés dans la liste déroulante. En cliquant sur le bouton **Tester l'accès à l'annuaire** au dessous, une fenêtre vous précisera si votre serveur principal est opérationnel. Vous pourrez cliquez sur **OK**.

Vous pouvez cliquer sur **Appliquer** pour valider votre configuration.

ONGLET « STRUCTURE»

Accès en lecture

Filtre de sélection des utilisateurs	Lors de l'utilisation du firewall en interaction avec une base externe, seuls les utilisateurs correspondants au filtre seront utilisés. Par défaut ce filtre correspond à *ObjectClass* = *InetOrgPerson*.
Filtre de sélection des groupes d'utilisateurs	Lors de l'utilisation du firewall en interaction avec une base externe, seuls les Groupes d'utilisateurs correspondants au filtre seront utilisés. Par défaut ce filtre correspond à *ObjectClass* = *GroupOfNames*.
Branche de l'autorité de certification	Ce champ définit l'emplacement de l'autorité de certification présente dans la base LDAP externe. Cet emplacement est notamment utilisé lors de la recherche de la CA utilisé pour la méthode d'authentification SSL. **NOTE** Il n'est pas indispensable de configurer ce champ mais dans ce cas, pour que la méthode d'authentification SSL fonctionne, il faut spécifier la CA dans la liste des CA de confiance dans la configuration de la méthode SSL. (Voir menu `Utilisateurs`\module `Authentification`\onglet `Méthodes disponibles` : il faut ajouter la méthode d'authentification **Certificat (SSL)** et indiquer la CA dans la colonne de droite « Autorités de confiance (C.A) »)

Correspondance d'attributs

Appliquer un modèle : Ce bouton vous propose de choisir parmi 3 serveurs LDAP, celui que vous appliquerez pour définir vos attributs :

- OpenLDAP
- Microsoft Active Directory (AD)
- Open Directory

Attributs de l'annuaire externe	Cette colonne représente la valeur donnée à l'attribut au sein de l'annuaire externe. **Exemples :** *Cn= NETASQ* *telephoneNumber= +33 (0)3 61 96 30* *mail = salesadmin@netasq.com*

L'annuaire est en lecture seule. La création d'utilisateurs et de groupes ne sera pas autorisée :
Si cette case est cochée, vous ne pourrez effectuer aucune action d'écriture.

Accès en écriture

Branche 'utilisateurs'	Donnez le nom de la branche LDAP pour stocker les utilisateurs. **Exemple** ou=users
Branche 'groupes'	Donnez le nom de la branche LDAP pour stocker les groupes d'utilisateurs. **Exemple** ou=groups.

Configuration avancée

Caractères protégés	Pour certains serveurs externes, il est nécessaire d'ajouter un \ pour que les requêtes LDAP soient comprises.

Hachage des mots de passe : La méthode de chiffrement des mots de passe des nouveaux utilisateurs.

Certaines méthodes d'authentification (comme LDAP) doivent stocker le mot de passe utilisateur sous la forme d'un hash (résultat d'une fonction de hachage appliquée au mot de passe) qui évite le stockage en clair de ce mot de passe.
Vous devez choisir la méthode de hash désirée parmi :

SHA	« Secure Hash Algorithm ». Cette méthode de chiffrement permet d'établir une chaîne de caractères de 160 bits ou octets (appelé « clé ») qui sert de référence pour l'identification.
MD5	« Message Digest ». Cet algorithme permet de vérifier l'intégrité des données saisies, en générant une « clé MD5 », de 128 bits. **REMARQUE** Cette méthode possédant un nombre d'octets moins élevé, et par conséquent, un niveau de sécurité plus faible, celle-ci est moins robuste aux attaques.
SSHA	« Salt Secure Hash Algorithm ». Repose sur le même principe que SHA, mais contient en plus une fonction de « salage » de mot de passe, qui consiste à ajouter une séquence de bit aux données saisies, afin de les rendre encore moins lisibles. **NOTE** Cette variante de SHA utilise une valeur aléatoire pour diversifier l'empreinte du mot de passe. Deux mots de passe identiques auront ainsi deux empreintes différentes. Cette méthode de chiffrement est la plus sécurisée et son utilisation est fortement recommandée.
SMD5	« Salt Message Digest ». Repose sur le même principe que MD5, avec la fonction de salage de mot de passe en plus.
CRYPT	Le mot de passe est protégé par l'algorithme CRYPT, dérivé de l'algorithme DES permettant le chiffrement par bloc, en utilisant des clés de 56 bits. Il est peu conseillé, possédant un niveau de sécurité relativement faible.
Aucune	Pas de chiffrement du mot de passe, celui-ci est stocké en clair. **AVERTISSEMENT** Cette méthode est très peu recommandée car vos données ne sont pas protégées.

Vous pouvez cliquer sur **Appliquer** pour valider votre configuration.

CONSOLE CLI

Ce module va vous permettre de visualiser les commandes exécutables de la console CLI (Command-Line Interface) de votre boîtier.
Vous pouvez y accéder en vous rendant au sein du menu `Système\Console CLI`.
Celui-ci est composé de deux parties :

- la liste des commandes en haut de l'écran, soit une zone de texte
- une zone de saisie des commandes en bas de l'écran

La liste des commandes

L'écran affiche par défaut, les 16 principales commandes exécutables qui font partie de la catégorie « HELP ».



NOTE
En saisissant la commande « HELP » dans la zone de saisie que nous traiterons ci-après, la liste résumant les commandes principales se réaffichera.

Les commandes visibles sont les suivantes :

AUTH	Utilisée dans le but d'éviter l'usurpation d'identité, cette commande permet à l'utilisateur ou l'administrateur de s'authentifier en toute sécurité.
CHPWD	Permet de redéfinir le mot de passe si nécessaire.
CONFIG	Permet d'accéder aux fonctions de configuration du firewall, regroupant 38 commandes implicites (CONFIG ACTIVATE, CONFIG ANTISPAM etc., cf « La zone de saisie »).
GLOBALADMIN	Permet d'obtenir des informations sur le système et comprend deux commandes implicites : GETINFOS et GETSTATUS.
HA	Permet d'accéder aux fonctions de la Haute Disponibilité, regroupant 8 commandes.
HELP	Cette commande, comme dit précédemment, permet d'afficher la liste des commandes exécutables principales.
LIST	Affiche la liste des utilisateurs connectés, en montrant les droits utilisateurs (par niveau) et les droits pour la session en cours (SessionLevel).
LOG	Permet d'afficher de consulter les journaux d'activités du firewall multifonction NETASQ, regroupant 6 commandes.
MODIFY	Cette commande est un droit spécifique permettant à l'utilisateur de modifier la configuration d'un module, en plus de la lecture.
MONITOR	Permet d'accéder aux fonctions relatives au MONITOR, contenant 20 commandes.
NOP	Aucune action ne sera effectuée, tout en évitant la déconnexion du serveur.
PKI	Permet d'afficher ou de télécharger la PKI, regroupant 7 commandes.
QUIT	Permet de se déconnecter.
SYSTEM	Regroupe les 20 commandes relatives au système.
USER	Regroupe les 12 commandes relatives à l'utilisateur.
VERSION	Permet d'afficher la version du serveur.

La zone de saisie

Lorsque vous vous rendez dans le module `Console CLI`, le focus est placé sur la zone de saisie des commandes.

A droite de celle-ci, deux boutons et une case à cocher permettent d'impacter certaines actions :

Exécuter	Ce bouton permet de lancer la commande saisie manuellement. La commande est également lancée lorsque l'utilisateur appuie sur « Entrée ».  **NOTE** Au sein de la cellule d'édition de la commande, vous pouvez naviguer à travers les différentes commandes déjà exécutées grâce aux touches fléchées du clavier Haut/Bas. L'historique des commandes est stocké et ré-utilisé à chaque fois que l'application web sera relancée.
Effacer l'affichage	Ce bouton permet d'effacer la liste de commandes affichée au-dessus (cf « La liste des commandes »). Pour la rendre visible de nouveau, entrez la commande HELP dans la zone de saisie et cliquez sur « Exécuter ».
Format brut	Si vous cochez cette case, l'exécution de la commande affichera en brut la ligne de code entre balises.

 **NOTE**

La plupart des commandes affichées dans la liste en haut de page en implique d'autres. Pour visualiser l'ensemble de ces commandes, procédez comme suit :

1. Entrez la commande de votre choix dans la zone de saisie de texte.
2. Cliquez sur « Exécutez ».
3. Selon la commande que vous avez choisie, la liste affichera les commandes supplémentaires inclus dans celle-ci.

Exemple

Si vous saisissez la commande CONFIG, toutes les commandes relatives à celle-ci apparaitront à l'écran.
Pour utiliser l'une de ces commandes, entrez dans la zone de saisie « CONFIG », suivi d'un espace et de la commande voulue, comme : « CONFIG HA ».

DHCP

L'écran de configuration du service `DHCP` se compose de 5 onglets :

- **`Général`** : Activation du service DHCP selon 2 modes spécifiques : serveur ou relai.
- **`Paramètres du serveur`** (avec la mention « inactif » si l'option **Activer le service** est décochée dans l'onglet **`Général`** ou si le mode Relai est sélectionné dans l'onglet **`Général`**). Ce menu est réservé à la configuration des adresses des différents serveurs : "Passerelle", "DNS","E-mail" (**SMTP** et **POP**), "Horaire" (**NTP**), News et serveur TFTP. Ces adresses seront automatiquement envoyées aux stations pour qu'elles puissent contacter les serveurs correspondants.
- **`Plage d'adresses`** (avec la mention « inactif » si le mode Relai est sélectionné dans l'onglet **`Général`**). Par plage, vous spécifiez un groupe d'adresses destinées à être allouées aux utilisateurs. L'adresse allouée l'est alors pour le temps déterminé dans la configuration globale.
- **`Machine`** (avec la mention « inactif» si le mode Relai est sélectionné dans l'onglet **`Général`**). Par machine, l'adresse allouée par le service est toujours la même : celle indiquée dans le menu **`Machine`**. Il s'agit en réalité d'un adressage "statique" mais qui permet de "libérer" le poste client de sa configuration réseau.
- **`Paramètres du relai`** (avec la mention « inactif » si le mode Relai n'a pas été sélectionné dans l'onglet **`Général)`**.

L'onglet « Général»

Activer le service : Active ou désactive les champs en mode « Serveur » ou en mode « Relai ».

Serveur DHCP	Envoie différentes configurations serveurs aux clients DHCP. Ces serveurs seront utilisés seulement si le logiciel client DHCP le réclame. En cochant cette option, l'onglet `Paramètres du relai` passe en mode « inactif ».
Relai DHCP	Le relai DHCP est à utiliser lorsque l'on souhaite rediriger les requêtes clientes vers un serveur DHCP externe. En cochant cette option, les onglets `Paramètres du serveur`, `Plage d'adresses` et `Machine` passent en mode « Inactif ».

L'onglet « Paramètres du serveur»

Il est possible ici de configurer des paramètres globaux, comme le **nom de domaine** que les machines vont utiliser, les **serveurs DNS**, etc.…

Nom de domaine	Nom de domaine utilisé pour la définition des utilisateurs.
Passerelle par défaut	La passerelle par défaut est la route par défaut utilisée si aucune autre n'a été spécifiée pour l'adresse du client ou du réseau.

Serveur DNS primaire et Serveur DNS secondaire	Envoie les adresses des serveurs DNS primaire et secondaire aux clients DHCP. Ces serveurs sont obligatoires dans presque chaque configuration DHCP. Si le firewall obtient l’adresse IP d’une de ses interfaces par DHCP, il est possible de définir les serveurs DNS obtenus par le firewall auprès du fournisseur d’accès. Pour ce faire, activer l’option **Demander les serveurs DNS au serveur DHCP et créer les objets machines associés** dans le module `Réseau\Interfaces\Configuration avancée` pour l’interface concernée. Ensuite, utiliser les objets « Firewall_<nom de l’interface>_dns1 » et « Firewall_<nom de l’interface>_dns2 » dans ces champs.

Configuration avancée

Serveur WINS	Envoie l’adresse du serveur WINS aux clients DHCP. WINS est un serveur de nom NETBIOS Microsoft (NBNS). WINS élimine le besoin de diffusion de données afin de résoudre les noms machines en fonction de leur adresse IP.
Serveur SMTP	Le serveur SMTP est utilisé pour envoyer des e-mails. Un clic à droite du champ permet de sélectionner le serveur.
Serveur POP3	le serveur POP3 est utilisé pour recevoir des e-mails. Un clic à droite du champ permet de sélectionner le serveur.
Serveur de temps (NTP)	Ce champ permet d'envoyer l'adresse du serveur NTP aux clients DHCP. Si les clients sont configurés pour synchroniser leur horloge NTP, ce serveur doit être utilisé comme une référence de temps.
Serveur de News (NNTP)	Ce champ permet d'envoyer l'adresse du serveur de news aux clients DHCP. Ce serveur fournit le service NNTP, qui autorise les clients à lire les nouvelles Usenet.
Serveur TFTP	Le serveur TFTP sert pour le boot à distance des machines. Ce champ peut être utilisé pour le démarrage d’équipements réseaux tels que des routeurs, des X-terminals ou des stations de travail sans disque dur.
Annoncer le fichier de configuration automatique des proxies (WPAD)	Permet au serveur de distribuer aux clients DHCP qui demandent une adresse, la configuration du proxy à travers le fichier PAC. Le fichier .PAC est transmis dans la réponse DHCP (champ option 252 : WPAD-URL). En cochant cette option, l’utilisateur sera informé qu’il devra activer le partage sur les interfaces internes et/ou externes dans l’écran d’authentification. *(Cf. Authentification).*
Mettre à jour les entrées des serveurs DNS	Coché par défaut. Mise à jour dynamique du DNS. Lorsque les informations contenues par le serveur DHCP sont modifiées, le serveur DNS primaire est dynamiquement mis à jour.

Durée de bail attribuée

Par défaut (heure)	Pour des raisons d’optimisation des ressources réseau, les adresses IP sont délivrées pour une durée limitée. Il faut donc indiquer ici le temps par défaut pendant lequel les stations garderont la même adresse IP.
Minimum (heure)	Temps au minimum pendant lequel les stations garderont la même adresse IP.
Maximum (heure)	Temps au maximum pendant lequel les stations garderont la même adresse IP.

L'onglet « Plage d'adresses»

NOTE GENERALE

A partir de cet onglet, vous rencontrerez cette icône qui vous permettra d'**Ajouter** des éléments à vos tableaux, et celle-ci pour les **Supprimer**

Pour qu'un serveur DHCP fournisse des adresses IP, il est nécessaire de lui donner un réservoir d'adresses dans lequel il pourra puiser.

Plages d'adresses	Il est possible de dire au serveur de ne fournir des adresses IP que dans les plages d'adresses définies par les lignes « dhcp_range » de cette colonne. Pour ce faire, choisir un « range » dans la base objet de la liste déroulante, en vous plaçant à droite de la cellule et en cliquant sur la flèche.
Passerelle	Si la passerelle associée à la plage d'adresses définie est « auto », c'est la passerelle par défaut qui sera utilisée. Vous pouvez en définir une autre en la sélectionnant dans la base objets, affichable en cliquant sur la flèche à droite de la cellule.

AVERTISSEMENTS

Deux plages ne peuvent se chevaucher. Une plage d'adresses appartient à un unique bridge/interface. Une machine ne peut être définie dans une plage. La passerelle définie pour un réseau appartient à ce réseau.

L'onglet «Machine»

L'onglet **`Machine`** permet de déclarer les machines que le DHCP doit connaître et leur appliquer une configuration particulière.
Dans cet onglet, il est possible de définir une adresse IP et une passerelle par défaut. Cette configuration se rapproche d'un adressage statique mais rien n'est indiqué sur le poste client. Ainsi la gestion des adresses allouées et de la configuration des postes clients est simplifiée.

La grille affiche la machine et la passerelle, cliquez sur la flèche à droite de chaque cellule pour sélectionner un objet dans la base.

AVERTISSEMENTS

Vous devez choisir un objet pour lequel une adresse MAC a été configurée.

L'adresse IP ne doit pas faire partie du plan d'adressage défini dans l'onglet `Plage d'adresses`.
L'adresse IP doit faire partie de la plage d'adresses de la/des interface(s) du firewall qui délivre(nt) des adresses IP en DHCP.

L'onglet « Paramètres du relai»

Le relai DHCP est utilisé si vous souhaitez rediriger les requêtes clientes vers un serveur DHCP externe.

Serveur(s) DHCP	Choix de l'adresse IP du relai DHCP.
Relayer les requêtes DHCP pour toutes les interfaces protégées	Le relai écoute sur toutes les interfaces protégées.

Interfaces d'écoute du service DHCP relai

Ajout et suppression des interfaces impliquées dans le relai.

AVERTISSEMENTS

Les interfaces d'écoute doivent comprendre les interfaces pour l'écoute de la requête côté client ainsi que les interfaces d'écoute de la réponse côté serveur.
Il faudra configurer le serveur DHCP de telle manière qu'il puisse distribuer des adresses IP aux clients qui passent à travers le relai.

DNS DYNAMIQUE

L'écran de configuration du client DNS dynamique se décompose en 2 parties :

- Sur la gauche, la « Liste des profils DNS dynamique ».
- Sur la droite, la « Résolution DNS », ou configuration du profil préalablement sélectionné.

Liste des profils DNS dynamique

Le tableau présentant les profils se compose de 2 colonnes :

Etat	Permet, par un double-clic d'activer ou de désactiver le profil.
Aperçu	Indications du nom du domaine, de l'interface et de l'état de la résolution associées au profil.

Le bouton **Ajouter** permet d'ajouter un profil.
Le bouton **Supprimer** permet de supprimer un profil préalablement sélectionné.

Configuration d'un profil

Résolution DNS

Nom de domaine (obligatoire)	Nom de domaine attribué au client DNS dynamique. Par exemple : *monfirewall.dyndns.org*. En utilisant l'option **Effectuer la résolution DNS pour les sous-domaines (gestion du wildcard),** vous pouvez couvrir tous les sous-domaines. Par exemple si vous spécifiez **netasq.dyndns.org** dans le champ "Nom de domaine" et que l'option **Effectuer la résolution DNS pour les sous-domaines (gestion du wildcard)** est sélectionnée, tous les sous-domaines (commerce.netasq.dyndns.org, labo.netasq.dyndns.org, etc.) seront associés au client.
Interface associée au nom de domaine	Nom de l'interface réseau dont l'adresse IP est associée au nom de domaine.  **NOTE** - Une interface ne peut utiliser qu'un seul profil. - Un profil ne peut être utilisé que par une interface. - Le profil ne peut être actif si une interface n'est pas indiquée
Effectuer la résolution DNS pour les sous-domaines (gestion du wildcard)	Active ou désactive la prise en compte des sous-domaines liés au nom de domaine.  **NOTE** Une souscription à l'offre Wildcard est nécessaire pour bénéficier de cette fonctionnalité.

Fournisseur du service DNS dynamique

Cette zone vous permet de saisir les informations d'accès de votre fournisseur de service DNS Dynamique.

Fournisseur DNS dynamique (obligatoire)	Fournisseur de services DNS. Actuellement, un seul fournisseur de services DNS est supporté : **DynDNS**.
Nom d'utilisateur (obligatoire)	Utilisateur indiqué par le fournisseur de services DNS pour l'authentification du client DNS dynamique.
Mot de passe (obligatoire)	Mot de passe indiqué par le fournisseur de services DNS pour l'authentification du client DNS dynamique.
Serveur DNS dynamique (obligatoire)	Serveur du fournisseur de services DNS. L'objet à spécifier dans ce champ doit obligatoirement se nommer : "members.dyndns.org" ou « members.dyndns.com » pour fonctionner avec Dyn DNS.
Service DNS dynamique (obligatoire)	Cette option vous permet d'indiquer le service que vous avez souscrit auprès de votre fournisseur de services DNS parmi "dynamic DNS", "custom", et "static DNS".

Configuration avancée

Des paramétrages de configuration avancée sont disponibles en cliquant sur le bouton **Configuration avancée**. Ils permettent notamment de renouveler l'enregistrement du changement d'adresse.

Fréquence de renouvellement (jour)	Période de renouvellement du service DNS dynamique. Cette période est fixée à 28 jours par défaut par NETASQ. **REMARQUE** **DynDNS** punit les renouvellements abusifs (fermeture du compte…). Ainsi un renouvellement survenu avant 26 jours (après le dernier renouvellement) n'est pas permis par **Dyn DNS** De plus sans renouvellement au delà de 35 jours, le compte est clôturé. Ces informations sont toutefois susceptibles d'être modifiées étant donné qu'il s'agit d'un fonctionnement établi par **Dyn DNS**.
Protocole utilisé pour la mise à jour	Protocole utilisé lors de la phase de renouvellement du service DNS dynamique. Les choix possible sont : HTTPS et HTTP.
Signaler au serveur DNS dynamique lorsque l'interface est inactive	Ce service payant chez **Dyn DNS** permet de rediriger les flux à destination de votre réseau vers une page spécifique lorsque votre connexion n'est pas en activité.

DROITS D'ACCES

Ce module se compose de 3 onglets :

- **`Options par défaut`** : Cet onglet vous permet de définir les accès VPN SSL, IPSEC ainsi que la méthode d'Authentification par défaut.
- **`Configuration par utilisateur`** : Grille de règles correspondant aux accès VPN SSL, IPSEC et d'Authentification des utilisateurs et groupes d'utilisateurs.
- **`PPTP`** : Permet d'ajouter et de lister les utilisateurs ayant accès au VPN PPTP par leur login, et de leur créer un mot de passe pour se connecter.

Onglet « Accès par défaut »

Authentification

Méthode par défaut	Ce champ vous permet de définir la méthode d'authentification par défaut pour les utilisateurs ou de Bloquer l'accès afin qu'ils ne puissent pas s'identifier. Vous visualisez dans la liste déroulante, les méthodes d'authentification que vous avez ajoutées et activées au préalable au sein du menu `Utilisateurs\Authentification\onglet Méthodes disponibles` (Certificat SSL, LDAP, Radius, SPNEGO, Kerberos).

Vous pouvez cliquer sur **Appliquer** pour valider votre configuration.

VPN SSL

Les profils VPN SSL (voir `menu VPN\module VPN SSL`) représentent l'ensemble de serveurs web et applicatifs que vous souhaitez lister afin de les attribuer à vos utilisateurs ou groupes d'utilisateurs.

Profil VPN SSL par défaut	Ce champ permet de définir le profil VPN SSL par défaut pour les utilisateurs. Vous devez avoir restreint au préalable l'accès aux serveurs définis dans la configuration du VPN SSL au sein du menu `VPN\VPN SSL`\onglet `Profils utilisateurs` (voir document VPN SSL). La liste déroulante laisse apparaître les options suivantes : Aucun profil : Les utilisateurs n'ont pas accès au VPN SSL. Accès à tous les profils : L'utilisateur a accès à tous les profils VPN SSL créés au préalable. ---------------------------------- <Nom du profil utilisateur1> : l'utilisateur aura uniquement accès à ce profil VPN SSL. <Nom du profil utilisateur2> : l'utilisateur aura uniquement accès à cet autre profil VPN SSL.

Vous pouvez cliquer sur **Appliquer** pour valider votre configuration.

IPSEC

Le VPN IPSec permet d'établir un tunnel sécurisé (authentification du correspondant, chiffrement et/ou vérification de l'intégrité des données) entre deux machines, entre une machine et un réseau, ou entre deux réseaux.

Politique IPSEC par défaut	Ce champ permet d'**Interdire** ou d'**Autoriser** par défaut des utilisateurs à négocier des tunnels VPN IPSec. Selon votre choix, les utilisateurs et les groupes d'utilisateurs pourront ou non en interne, communiquer sur vos réseaux IP privés et protégés, permettant ainsi le transport sécurisé de leurs données.

Vous pouvez cliquer sur **Appliquer** pour valider votre configuration.

Onglet « Politique d'accès »

Les manipulations possibles

Bouton **Ajouter** : Insérer une ligne à configurer après la ligne sélectionnée.
Bouton **Supprimer** : Supprimer la ligne sélectionnée.
Bouton **Monter** : Placer la ligne sélectionnée avant la ligne directement au dessus.
Bouton **Descendre** : Placer la ligne sélectionnée après la ligne directement en dessous.

A partir de la version 9.0.1, un champ de recherche par mots/lettres clés permet d'accéder aux utilisateurs souhaités.

La grille de configuration

Elle va vous permettre d'accorder ou non des droits d'accès à vos utilisateurs ou groupes d'utilisateurs. Vous pouvez les personnaliser au niveau de l'Authentification, du VPN SSL et de l'IPSEC.
La grille présente les colonnes suivantes :

Etat	Etat de la configuration des droits d'accès de l'utilisateur ou du groupe d'utilisateurs : Activé : Double-cliquez un point de la colonne pour activer la règle créée. Désactivé : La règle n'est pas opérationnelle. La ligne sera grisée afin de refléter la désactivation.  **REMARQUE** Le firewall va évaluer les règles dans leur ordre d'apparition à l'écran : une à une en partant du haut, celles-ci sont d'ailleurs numérotées à gauche de la colonne. Si la règle 1 concerne un groupe d'utilisateur, chaque utilisateur attaché aux règles suivantes et faisant partie de ce même groupe sera soumis à sa configuration. **Exemple** : Si vous interdisez l'authentification et/ou l'accès au VPN SSL à un groupe en règle 1, et que l'utilisateur en règle 2 peut s'authentifier via le LDAP et à un profil VPN SSL particulier et fait partie du groupe, celui-ci sera bloqué, et n'aura accès ni à l'authentification, ni au VPN SSL.
Utilisateur –	Lorsqu'une nouvelle ligne est ajoutée à la grille, vous pouvez sélectionner l'utilisateur

groupe d'utilisateurs	ou le groupe d'utilisateur pour lequel vous souhaitez effectuer une configuration. Pour cela, cliquez sur la flèche à droite de la colonne, une liste déroulante s'affiche et vous propose de choisir parmi les CN créés précédemment, au sein du menu `Utilisateurs\module Utilisateurs`. **NOTE** Il est également possible d'ajouter un utilisateur qui ne figure pas dans la base LDAP, par exemple, pour la méthode KERBEROS ou RADIUS.
Authentification	Cette colonne déroule la liste des choix d'authentification possibles pour votre utilisateur ou groupe d'utilisateurs. Vous ne pourrez visualiser que les méthodes d'authentification que vous avez autorisées au sein du menu `Utilisateurs\module Authentification\onglet Méthodes disponibles` (cf document sur l'`Authentification`).  **NOTE** Si vous n'avez effectué aucune configuration préalable de méthode d'authentification, seul « Défaut » et « Interdire » vous seront proposées lorsque vous cliquerez sur la flèche à droite de la colonne. En sélectionnant « Défaut », la méthode choisie d'office sera celle que vous avez définie dans l'onglet précédent `Options par défaut\`champ `Authentification- Méthode par défaut.` En sélectionnant « Interdire », l'utilisateur ou groupe d'utilisateur choisi ne pourra pas s'authentifier.
SSL VPN	Cette colonne vous permet d'attribuer un profil VPN SSL en particulier à un utilisateur ou à un groupe d'utilisateur, préalablement configuré au sein du menu VPN\module VPN SSL\onglet Profils utilisateurs. Vous pouvez également sélectionner l'option Défaut, qui prendra en compte le profil VPN SSL par défaut saisi dans l'onglet précédent (Options par défaut). Si vous choisissez Interdire, l'utilisateur ou groupe d'utilisateur n'aura accès à aucun profil VPN SSL, à l'inverse de l'option Tous les profils qui ouvrira l'accès à tous les serveurs web et applicatifs activés au sein des profils utilisateurs.
IPSEC	Ce champ permet d'Interdire ou d'Autoriser des utilisateurs à négocier des tunnels VPN IPSec. Selon votre choix, les utilisateurs et les groupes d'utilisateurs pourront ou non en interne, communiquer sur vos réseaux IP privés et protégés, permettant ainsi le transport sécurisé de leurs données.  **REMARQUE** Le droit IPSEC ne concerne que les tunnels : avec authentification par clé pré-partagée et des identifiants de type e-mail ou avec authentification par certificat.
Description	Commentaire éventuel décrivant l'utilisateur, le groupe d'utilisateur ou la règle.

 **REMARQUE**

Lorsque vous ajoutez une ligne au tableau et que vous n'avez encore mis en place aucune règle, les colonnes **Authentification**, **VPN SSL** et **IPSEC** sont en « Interdire » par défaut, même si vous les avez configurées différemment au sein de l'onglet Options par défaut.

Il faut donc cliquer sur l'option « Défaut » à l'aide de la flèche de droite dans chaque colonne si vous souhaitez récupérer vos modifications effectuées préalablement.

Onglet « Serveur PPTP »

Il permet de lister les utilisateurs ayant accès au `VPN PPTP`, leur donnant accès à une connexion sécurisée et chiffrée pour leur login.

Vous pouvez effectuer les actions suivantes :

Ajouter	Lorsque vous cliquez sur ce bouton, une nouvelle ligne vient s'ajouter au tableau et vous présente la liste déroulante des utilisateurs créés au préalable au sein du menu `Utilisateurs\module Utilisateurs`: Pour que l'opération soit valide, vous devez entrer le mot de passe de l'utilisateur dans la fenêtre qui s'affiche. **NOTE** Il est possible de saisir un utilisateur ne figurant pas dans la base des utilisateurs du firewall, le PPTP étant indépendant du module LDAP.
Supprimer	Sélectionner la ligne contenant l'utilisateur à retirer de la liste des login PPTP, puis cliquer sur **Supprimer**.
Modifier le mot de passe	Sélectionner la ligne contenant l'utilisateur dont vous souhaitez modifier le mot de passe et entrez les nouvelles données dans la fenêtre qui s'affiche.

ENROLEMENT

Le service d'enrôlement web NETASQ permet à un utilisateur "inconnu" à la base des utilisateurs de demander la création de son compte d'accès (à Internet, au serveur mail, à tous les services qui nécessitent une authentification) et de son certificat.

Ce module requiert au minimum de l'utilisation d'une base LDAP pour les requêtes utilisateurs et d'une autorité racine (PKI interne) pour les demandes de certificats utilisateur.

L'écran du module `Enrôlement` se compose de 3 zones :

- La grille contenant les demandes d'enrôlement des utilisateurs et des certificats à gauche
- Les informations relatives à l'utilisateur ou au certificat sélectionné à droite
- Les propriétés avancées

La grille d'enrôlement

Les actions possibles

Approuver	Lorsqu'un utilisateur fait une demande d'enrôlement ou de certificat, la requête est entrée dans une grille. Pour valider la demande de l'utilisateur, positionnez-vous sur la ligne correspondante et cliquez sur **Approuvez**.
Rejeter	Vous pouvez également refuser la demande d'enrôlement ou de certificat d'un utilisateur en sélectionnant la ligne correspondante et en cliquant sur le bouton **Rejeter**.
Ignorer	Ce bouton permet d'annuler l'action approuvée ou rejetée. Cela évite d'utiliser le bouton **Annuler** et d'effacer les opérations en cours.
Actualiser	Ce bouton permet de rafraîchir la liste des demandes d'enrôlement ou de certificats. De cette façon, toute requête récente sera automatiquement ajoutée à la grille, en attente de sa validation ou de son refus.

Les demandes d'enrôlement utilisateurs et certificats

Type	Cette colonne indique le type de requête créée par l'utilisateur : une demande d'enrôlement caractérisée par « **Utilisateur** » ou une demande de « **Certificat** ».
CN utilisateur	Le nom permettant d'identifier l'utilisateur ou le certificat.
E-mail	L'adresse e-mail de l'utilisateur qui permettra de lui envoyer une validation ou un refus de sa demande d'enrôlement ou de certificat.

Le formulaire récapitulatif

Il renseigne les informations de la ligne utilisateur/certificat sélectionnée.

Identifiant	Identifiant de connexion de l'utilisateur
Nom	Nom de l'utilisateur
Prénom	Prénom de l'utilisateur
E-mail	Adresse e-mail de l'utilisateur. Celle-ci sera utile pour lui envoyer une réponse concernant sa demande d'enrôlement ou de certificat.
Description	Description indicative à l'utilisateur
Téléphone	Coordonnées téléphoniques de l'utilisateur
Mot de passe	Mot de passe de l'utilisateur
Requête de certificat	Indique si l'utilisateur a effectué une requête de certificat au cours de sa demande d'enrôlement.

 **NOTE**
Pour le cas des demandes de certificats, seul le détail de l'adresse e-mail s'affiche dans le champ de droite.

Propriétés avancées

Activer automatiquement les requêtes de certificats

Cette option vous permet la validation automatique des requêtes de certificats. Lorsque l'administrateur valide la requête de création de compte utilisateur, l'application validera automatiquement la création du certificat associé à cet utilisateur.

<u>Format de l'identifiant utilisateur pour les ID vides</u>

Format de l'identifiant	Définissez une chaîne de caractères par défaut pour les identifiants de connexion. **Exemple :** %F.%L
Exemple	Exemple illustrant l'identifiant utilisateur. **Exemple :** JEAN.DUPONT

 **NOTE**
Il est possible de définir le nombre de caractère souhaité pour le prénom et/ou le nom en plaçant un chiffre après le F et/ou L
%F1%L
JDUPONT

<u>E-mails</u>

Envoyer un e-mail à l'utilisateur :
lors de l'approbation/rejet de sa requête d'enrôlement
Cette option permet l'envoi d'un e-mail à l'utilisateur pour l'informer de la validation ou du rejet de sa demande d'enrôlement.

lors de l'approbation/rejet de sa requête de certificat
Cette option permet l'envoi d'un e-mail à l'utilisateur pour l'informer de la validation ou du rejet de sa demande de certificat.

ÉVÉNEMENTS SYSTÈMES

Ce module va vous permettre de définir le niveau d'alerte des événements système divers pouvant apparaître au sein de vos configurations (attaques, échecs de mises à jour, CRL invalide etc.).
Il est composé d'un unique écran, listant les événements par numéro et par ordre alphabétique, avec la possibilité de rechercher un événement particulier.

Les actions possibles

Vous pouvez dans un premier temps, effectuer deux actions.

Rechercher

Cette zone de saisie permet la recherche par occurrence, lettre ou mot. Vous pouvez ainsi filtrer les éléments de la liste afin de n'afficher que ceux que vous souhaitez.
Exemple
Si vous saisissez « CRL » dans le champ, tous les messages comportant ce terme s'afficheront dans la grille.

Restaurer la configuration par défaut

Ce bouton va permettre d'annuler tous les changements que vous avez effectués au préalable au sein de la configuration des événements systèmes.
Lorsque vous cliquez sur ce bouton, un message de confirmation s'affiche, permettant de valider ou non l'action.

La liste des événements

L'écran est composé de trois colonnes, ainsi que d'une page d'aide disponible en bout de ligne pour chaque type d'événement.

Identifiant	Ce champ affiche le numéro permettant d'identifier l'événement. Il n'est pas éditable.
Niveau	Cette colonne affiche les niveaux d'alertes attribués aux événements par défaut. Il en existe 4, que vous pouvez modifier en sélectionnant le niveau désiré au sein de la liste déroulante, accessible en cliquant sur la flèche de droite : **Ignorer** : Aucune trace de l'événement ne sera conservée au sein des logs. **Mineur** : Dès que l'événement concerné est détecté, une alarme mineure est générée. Cette alarme est reportée dans les logs, et peut être envoyée par Syslog, (partie `Traces – Syslog`) ou par e-mail (voir module `Alertes e-mails`).

	Majeur : Dès que l'événement concerné est détecté, une alarme mineure est générée. Cette alarme est reportée dans les logs, et peut être envoyée par Syslog, (partie `Traces - Syslog`) ou par e-mail (voir module `Alertes e-mails`). **Tracer** : Le firewall NETASQ n'effectue aucune action. Ceci est utile si vous voulez juste tracer certains flux sans appliquer d'action particulière.
Message (langue dépendante du firewall)	Ce champ affiche le nom de l'événement système et ses caractéristiques et n'est pas éditable. **NOTE** En cliquant sur la flèche de droite en tête de la colonne, vous pouvez inverser l'ordre d'apparition des événements.
Afficher l'aide	Lorsque vous sélectionnez un événement au sein de la liste en positionnant votre curseur dessus, un lien « Afficher l'aide » apparait. En cliquant sur celui-ci, vous serez renvoyé sur la base de connaissances NETASQ, donnant plus de détails sur les informations relatives à l'événement.

NOTE GENERALE
Lorsque vous modifiez le niveau d'alerte d'un événement, n'oubliez pas de cliquer sur le bouton « Appliquer » en bas de la page, afin de valider votre action.

FILTRAGE ET NAT

Le Filtrage et le NAT sont désormais réunis en un seul module et font partie du menu Politique de Sécurité.

Ce nouveau module se compose de 2 onglets, comportant chacun un emplacement réservé aux politiques de filtrage et de NAT, et à leur configuration :

- Le Filtrage : Il s'agit d'un ensemble de règles qui laissent passer ou bloquent certains trafics réseaux suivant des critères définis.
- Le NAT : Il permet de faire de la réécriture (ou translation) d'adresses et de ports source et destination.

Les politiques

Le bandeau vous permet de sélectionner et de manipuler les politiques associés au Filtrage d'une part, et au NAT d'autre part.

Sélection de la politique de filtrage

Le menu déroulant propose 10 politiques de filtrage préconfigurées, numérotées de 1 à 10 :

« Block all (1) »	En sélectionnant cette politique, vous n'aurez accès qu'à l'écran d'administration du firewall quel que soit l'interface sur laquelle vous êtes connectés. Toutes les autres connexions seront bloquées.
« High (2) »	Si vous choisissez cette politique de filtrage, seuls les trafics web, e-mail, FTP, et les requêtes ICMP seront autorisés depuis les réseaux internes vers l'extérieur.
« Medium (3) »	En choisissant cette politique, la prévention d'intrusion sera effectuée sur les connexions sortantes, dans la mesure où le protocole peut être détecté automatiquement par le moteur de prévention des menaces : Par exemple, le port 80 est généralement utilisé pour faire du HTTP. Tout trafic sur le port 80 sera considéré comme du trafic HTTP par le firewall, car ce port est défini comme port par défaut pour le protocole HTTP (les ports par défaut pour chaque protocole sont défini depuis le menu Protection applicative \ Protocoles et applications). En revanche, si un autre protocole est utilisé (par exemple un tunnel ssh) à destination du port 80, la connexion sera alors déclarée illégitime et bloquée, car le seul protocole autorisé est l'HTTP.  **REMARQUE** Toutes les connexions sortantes TCP non-analysables (pour lesquelles aucune reconnaissance du protocole n'est possible) seront acceptées.
« Low (4) »	Une analyse des protocoles sera forcée pour les connexions sortantes.  **REMARQUE** Toutes les connexions sortantes non-analysables seront autorisées.

« Filter 05, 06, 07, 08, 09 »	Hormis les 5 politiques configurées par défaut (**Block all, High, Medium, Low, Pass all,** éditables si vous le souhaitez), 5 politiques vides à paramétrer vous-mêmes sont disponibles.
« Pass all (10) »	Cette politique laisse passer l'ensemble du trafic. Elle ne devrait être utilisée qu'à des fins de test.

NOTE

Vous pouvez **Renommer** ces politiques et modifier leur configuration dès que vous le souhaitez (voir ci-dessous).

Les actions

Activer la politique sélectionnée	Active immédiatement la politique en cours d'édition: Les paramètres enregistrés écrasent les paramètres en vigueur et la politique est appliquée immédiatement sur le firewall.
Editer	Cette fonction permet d'effectuer 3 actions sur les politiques : • **Renommer** : en cliquant sur cette option, une fenêtre composée de deux champs à remplir s'affiche. Celle-ci propose de modifier le nom de la politique de filtrage d'une part et d'ajouter un commentaire d'autre part. Une fois l'opération effectuée, cliquez sur « Mettre à jour ». Il est également possible d' « Annuler » la manipulation. • **Réinitialiser** : Permet de rendre au politique sa configuration initiale, de sorte que toutes les modifications apportées soient supprimées. • **Copier vers** : Cette option permet de copier un politique vers une autre, toutes les informations de la politique copiée seront transmises à la politique réceptrice. Il portera également le même nom.
Dernière modification	Cette icône permet de connaître la date et l'heure de la dernière modification enregistrée.

A partir de la version 9.0.1, les règles de filtrage et NAT peuvent être déplacées par glisser-déposer.

Le glisser-déposer (« drag'n'drop »)

Tout au long de votre création et édition de règle, il sera possible de glisser-déposer des objets et des actions.
Vous pourrez déplacer n'importe quel objet où vous le souhaitez dans la grille, ainsi qu'en insérer depuis votre barre de navigation à gauche (champ `Objets`), s'ils ont été préalablement créés (vous pouvez également les créer directement depuis chaque champ qui accepte un objet).

REMARQUE

Deux icônes vous permettront de savoir si l'objet ou l'action sélectionnée peut être déplacé au sein d'une cellule particulière :

Indique que l'opération est possible,

. Indique que l'objet ne peut être ajouté à la cellule choisie.

L'onglet « Filtrage »

La technologie de prévention d'intrusion NETASQ inclut un moteur de filtrage dynamique des paquets (« stateful inspection ») avec optimisation des règles permettant l'application de la politique de filtrage de manière sûre et rapide.
La mise en œuvre des fonctions de filtrage est basée sur la confrontation des attributs de chaque paquet IP reçu aux critères de chaque règle de la politique de filtrage actif. Le filtrage porte sur tous les paquets sans exception.

Les critères de sélection du trafic pour une règle de filtrage sont :

- L'interface de réception des paquets IP couverts par la règle.
- La ou les machines à l'origine des flux d'informations couverts par la règle.
- Le ou les protocoles IP, les services TCP/UDP ou les types de messages ICMP des flux d'information couverts par la règle, le DSCP afin de définir une différenciation des flux.
- La ou les machines destinataires des flux d'informations couverts par la règle.
- L'utilisateur ou le groupe d'utilisateurs autorisés par la règle.

Les attributs des paquets IP sont extraits des en-têtes IP, ICMP, UDP ou TCP des trames.
En ce qui concerne l'utilisateur ou le groupe d'utilisateurs autorisés par la règle, à partir du moment où un utilisateur s'est identifié et authentifié avec succès à partir d'une machine donnée, le firewall retient ce fait et attribue le nom de l'identifiant de cet utilisateur à tous les paquets IP en provenance de l'adresse de cette machine.

En conséquence, les règles qui spécifient l'authentification des utilisateurs, même sans préciser de contraintes sur les utilisateurs autorisés, ne peuvent s'appliquer qu'à des paquets IP émis d'une machine à partir de laquelle un utilisateur s'est préalablement authentifié. Chaque règle de filtrage peut spécifier une action de contrôle (voir colonne `Action`).

Le `Filtrage` est composé de deux parties. Le bandeau situé en haut de l'écran, permettant de choisir la politique de filtrage, de l'activer, de l'éditer et de visualiser sa dernière modification. La grille de filtrage est dédiée à la création et la configuration des règles.

Les actions sur les règles de la politique de filtrage

Rechercher	Ce champ permet la recherche par occurrence, lettre ou mot. **Exemple :** Si vous saisissez « Network_internals » dans le champ, toutes les règles de filtrage comportant « Network_internals » s'afficheront dans la grille.
Nouvelle règle	Insérer une ligne prédéfinie ou à définir après la ligne sélectionnée. 5 choix sont possibles, les règles d'authentification, d'inspection SSL et de proxy HTTP explicite seront définies via un assistant dans une fenêtre à part : - **Règle standard** : Cette option permet de créer une règle vide laissant à l'administrateur la possibilité de remplir les différents champs de la grille de filtrage. - **Séparateur – regroupement de règles** : Cette option permet d'insérer un séparateur au dessus de la ligne sélectionnée et contribue à améliorer la lisibilité et la visibilité de la politique de filtrage. Elle peut, par exemple, permettre à l'administrateur de hiérarchiser ses règles. Ou de regrouper celles qui régissent le trafic vers les différents serveurs. ***A partir de la version 9.0.1,*** vous pouvez copier/coller un séparateur d'un emplacement à une autre.

	Règle d'authentification : Cette option a pour but de rediriger les utilisateurs non authentifiés vers le portail captif. En la sélectionnant, un assistant d'authentification s'affiche. Vous devrez choisir la **Source** (affichant « Network_internals » par défaut) et la **Destination** (affichant « Internet » par défaut) de votre trafic parmi la liste déroulante d'objets, puis cliquer sur **Terminer.** **Règle d'inspection SSL** : Cet assistant de création de règles a pour but d'inspecter le trafic chiffré SSL. Vous devrez définir la **Politique du trafic à déchiffrer** en indiquant les **Machines sources** (« Network_internals » par défaut), l'**Interface d'entrée** (« any » par défaut), la Destination (« Internet » par défaut) et le Port de destination (« ssl » par défaut) parmi la liste déroulante d'objets. Afin **d'Inspecter le trafic déchiffré** via la seconde zone de la fenêtre de l'assistant, vous devrez définir la configuration du **Profil d'Inspection**, en choisissant l'une de celle que vous avez définie au préalable dans `Protection Applicative/Profil d'inspection`, ou laisser en mode « Auto ». Vous pouvez également sélectionner une **politique de filtrage SSL** (filtrage par le contenu du certificat SSL) ainsi que l'**Antivirus** et les activer(boutons **On**/ **Off**). **Règle de proxy HTTP explicite** : Cette option permet d'activer le proxy HTTP explicite et de définir qui peut y accéder. Vous devrez choisir un objet **Machines** et une **Interface d'entrée** via le champ « **Source** ». Définissez ensuite **l'Inspection du trafic relayé** en indiquant si vous souhaitez attribuer une configuration par défaut au `Filtrage URL` et à l'`Antivirus`, et les activer (boutons **On**/ **Off**). Cliquez ensuite sur **Terminer**.
Supprimer	Supprime la ligne sélectionnée.  **NOTE** Il est possible de supprimer plusieurs lignes en même temps, en les sélectionnant avec la touche « Ctrl » puis en cliquant sur **Supprimer**.
Monter	Placer la ligne sélectionnée avant la ligne directement au dessus.
Descendre	Placer la ligne sélectionnée après la ligne directement en dessous.
Copier	Ce bouton permet de copier une règle de filtrage dans le but de la dupliquer.
Coller	Ce bouton permet de dupliquer une règle de filtrage, après l'avoir copié.
Réinit. colonnes	Lorsque vous cliquez sur la flèche de droite dans le champ du nom d'une colonne (exemple : **Etat**), vous avez la possibilité d'afficher des colonnes supplémentaires ou d'en retirer afin qu'elles ne soient pas visibles à l'écran, grâce à un système de coche. **Exemple** : Vous pouvez cocher les cases « **Nom** » et « **Port src** » qui ne sont pas affichées par défaut. En cliquant sur le bouton **réinit. colonnes**, vos colonnes seront remises à leur état initial, avant que vous n'ayez coché de case additionnelle. Ainsi, les cases « **Nom** » et « **Port src** » seront de nouveau masquées.

La grille de filtrage

Elle vous permet de définir les règles de filtrage à appliquer. Ordonnez-les afin d'avoir un résultat cohérent : le firewall exécute les règles dans l'ordre d'apparition à l'écran (numérotées 1, 2 etc) et s'arrête dès qu'il trouve une règle correspondant au paquet IP.

Il convient donc de définir les règles dans l'ordre du **plus restrictif au plus général**.

NOTE GENERALE :

Chaque fois que vous rencontrerez une liste déroulante d'objets au sein des colonnes (exceptées « Etat » et « Action **»**) une icône d'opérateur de comparaison mathématiques apparaîtra ( ). Elle ne sera utilisable que si un autre objet que « **Any** » est sélectionné.

Vous pourrez ainsi personnaliser les paramètres de votre trafic par le biais de l'icône suivante de 4 manières différentes :

- « = » (ou): la valeur de l'attribut correspond à ce qui est sélectionné.
- « != » (ou) la valeur de l'attribut est différente de ce qui est sélectionné.
- « < » (ou ; utilisable pour les ports source et destination uniquement) : le numéro de port du trafic est inférieur à ce qui est sélectionné.
- « > » (ou ; utilisable pour les ports source et destination uniquement) : le numéro du port du trafic est supérieur à ce qui est sélectionné.

A partir de la version 9.0.1, si vous cliquez rapidement 10 fois sur le bouton "Monter", vous distinguez la règle monter visuellement mais la fenêtre d'attente n'apparaît que lorsqu'on ne touche plus au bouton au-delà de 2 ou 3 secondes. Et au final, une seule commande sera passée.



NOTE

Ceci rend le déplacement des règles beaucoup plus fluide.

La grille de filtrage présente les colonnes suivantes :

Etat

Cette colonne affiche l'état **On**/ **Off** de la règle. Double-cliquez dessus pour changer l'état : en effectuant cette manipulation une fois, vous activez la règle de filtrage. Renouvelez l'opération pour la désactiver.

Action

Cette zone désigne l'action appliquée sur le paquet remplissant les critères de sélection de la règle de filtrage.
Pour définir les différents paramètres de l'action, double-cliquez dans la colonne, une fenêtre contenant les éléments suivants s'affiche :

Onglet « Général »

Général

Action	Il est possible d'effectuer 5 actions différentes : **Passer** : Le firewall NETASQ laisse passer le paquet correspondant à cette règle de filtrage. Le paquet ne descend plus dans la liste de règles. **Bloquer** : Le firewall NETASQ bloque silencieusement le paquet correspondant à cette règle de filtrage : le paquet est supprimé sans que l'émetteur ne s'en aperçoive. Le paquet ne descend plus dans la liste des règles. **Déchiffrer** : Cette action permet de déchiffrer le trafic chiffré. Le flux déchiffré continue descend dans la liste des règles. Il sera de nouveau chiffré après l'analyse (si aucune règle ne le bloque).

	Tracer : Le firewall NETASQ n'effectue aucune action. Ceci est utile si vous voulez juste tracer certains flux sans appliquer d'action particulière. **Reinit. TCP/UDP**: Cette option concerne surtout les trafics TCP et UDP : Dans le cas d'un trafic TCP, un paquet « TCP reset » sera envoyé à l'émetteur de celui-ci. Dans le cas d'un trafic UDP, un paquet ICMP « port unreachable » sera envoyé à l'émetteur de celui-ci. En ce qui concerne les autres protocoles IP, le Firewall NETASQ bloque simplement le paquet correspondant à cette règle de filtrage. Si vous vous trouvez en mode d'édition de la politique globale de filtrage, une 6ème possibilité apparaît: « Déléguer ». Cette option permet de ne plus confronter le trafic au reste de la politique globale, mais de le confronter directement à la politique locale.
Niveau de trace	4 choix sont possibles : **Aucun** : Aucune trace n'est conservée si le paquet correspond à cette règle de filtrage.  **NOTE** Cette option est indisponible si vous avez préalablement choisi l'action « Tracer » au sein du champ précédent. **Tracer** : Si vous choisissez cette option, une trace sera ajoutée dans les logs de filtrage. **Alarme mineure** : Dès que cette règle est appliquée à une connexion, une alarme mineure est générée. Cette alarme est reportée dans les logs, et peut être envoyée par Syslog, (partie `Traces - Syslog`) ou par e-mail (voir module `Alertes e-mails`). **Alarme majeure** : Dès que cette règle est appliquée à une connexion, une alarme mineure est générée. Cette alarme est reportée dans les logs, et peut être envoyée par Syslog, (partie `Traces - Syslog`) ou par e-mail (voir module `Alertes e-mails`).
Programmation horaire	Afin de pouvoir utiliser ce champ, vous devez avoir créé au moins un Objet Temps au sein du menu `Objets`\module `Objets Temps`. Vous pourrez ainsi définir la **période/**le **jour de l'année/**le **jour de la semaine/** l'**heure/**la **récurrence** de validité des règles.
Routage	
Passerelle - routeur	Cette option est utile pour spécifier un routeur particulier qui permettra de diriger le trafic correspondant à la règle vers le routeur défini.  **NOTE** Au moment du traitement du paquet, le moteur de prévention d'intrusion NETASQ évalue les règles dans l'ordre où elles sont définies dans la grille.

Cliquer sur **Ok** pour valider votre configuration.

Onglet « Qualité de service »

Le module de `QoS`, intégré au moteur de prévention d'intrusion NETASQ est associé au module `Filtrage` pour offrir les fonctionnalités de Qualité de Service.
Dès sa réception ; le paquet est traité par une règle de filtrage puis le moteur de prévention d'intrusion l'affecte à la bonne file d'attente suivant la configuration du champ QoS de cette règle de filtrage.

QoS

File d'attente	Ce champ vous propose de choisir parmi les files d'attente que vous avez définies au préalable au sein du module `Qualité de service`, du menu `Politique de Sécurité`.
Répartition	**Pas de répartition** : Si vous choisissez cette option, aucune attribution particulière de bande passante ne sera effectuée et chaque utilisateur/machine/connexion l'utilisera en fonction de ses besoins. **Equité entre les utilisateurs** : la bande passante sera répartie équitablement entre les différents utilisateurs. **Equité entre les machines** : la bande passante sera répartie équitablement entre les différentes machines. **Equité entre les connexions** : la bande passante sera répartie équitablement entre les différentes connexions.

Seuil de connexion
Le firewall NETASQ peut limiter le nombre maximal de connexions acceptées par seconde pour une règle de filtrage. Il faut définir pour les protocoles correspondant à la règle (TCP, UDP, ICMP), le nombre désiré.

 **AVERTISSEMENT**
La limitation ne s'appliquera qu'à la règle correspondante.
Exemple
Si vous créez une règle HTTP, seule la limitation TCP sera prise en compte. Cette option vous permet aussi d'éviter le déni de service que pourrait tenter d'éventuels pirates : vous pouvez limiter le nombre de requêtes adressées à vos serveurs par seconde.

 **REMARQUE**
Si l'option est affectée à une règle contenant un groupe d'objets, la limitation s'applique au groupe dans son ensemble (nombre total de connexions).

Si le seuil est atteint	**Ne rien faire** : aucune limitation de connexion par seconde (c/s) ne sera établie. **Activer le proxy SYN** : Cette option permet de protéger les serveurs contre les attaques par saturation de paquets TCP SYN (« SYN flooding ») le proxy SYN répondra à la place du serveur et évaluera la fiabilité de la requête TCP, avant de la transmettre. Vous pourrez limiter le nombre de connexions TCP par secondes pour cette règle de filtrage dans le champ en dessous. **Bloquer le trafic** : Selon le nombre maximum de connexions par seconde que vous attribuerez aux protocoles ci-dessous, le trafic sera bloqué une fois que le nombre défini sera dépassé.
TCP (c/s)	Nombre de connexions maximum par seconde autorisé pour le protocole TCP.
UDP (c/s)	Nombre de connexions maximum par seconde autorisé pour le protocole UDP.
ICMP (c/s)	Nombre de connexions maximum par seconde autorisé pour le protocole ICMP.

Cliquer sur **Ok** pour valider votre configuration.

DSCP

Le DSCP (*Differentiated Services Code Point)* est un champ dans l'entête d'un paquet IP. Le but de ce champ est de permettre la différentiation de services contenus dans une architecture réseau. Celle-ci spécifie un mécanisme pour classer et contrôler le trafic tout en fournissant de la qualité de service (QoS).

Forcer la valeur	En cochant cette case, vous dégrisez le champ du dessous et libérez l'accès au service DSCP. Cette option permet de réécrire le paquet avec la valeur donnée, afin que le routeur suivant connaisse la priorité à appliquer sur ce paquet.
Nouvelle valeur DSCP	Ce champ permet de définir une différenciation des flux. Via celui-ci, il est possible de déterminer grâce à un code préétabli, l'appartenance d'un trafic à un certain service plutôt qu'à un autre. Ce service DSCP, utilisé dans le cadre de la Qualité de Service, permet à l'administrateur d'appliquer des règles de QoS suivant la différenciation des services qu'il aura définis.

Cliquer sur **Ok** pour valider votre configuration.

Configuration avancée

Service	**Aucun** : Cette option implique qu'aucun des trois services suivants ne sera utilisé: l'utilisateur ne passera pas par le proxy HTTP et ne sera pas redirigé vers la page d'authentification. **Proxy HTTP :** Si vous choisissez cette option, les connexions des utilisateurs seront interceptées par le proxy HTTP qui analysera le trafic de manière transparente. **Authentification** : Si vous choisissez cette option, les utilisateurs non authentifiés seront redirigés vers le portail captif lors de leur connexion.
Compter	Si vous cochez cette case, le firewall NETASQ comptera le nombre de paquets correspondants à cette règle de filtrage et génèrera un rapport. Il est ainsi possible d'obtenir des informations de volumétrie sur les flux désirés.

Cliquer sur **Ok** pour valider votre configuration.

Source

Ce champ désigne la provenance du paquet traité, il est utilisé comme critère de sélection pour la règle. Un double-clic sur cette zone permettra de choisir la valeur associée dans une fenêtre dédiée. Celle-ci comporte deux onglets :

Onglet « Général »

Général

Utilisateur	La règle s'appliquera à l'utilisateur que vous sélectionnerez dans ce champ. Il en existe deux par défaut : **« Any user »** : désigne tout utilisateur authentifié. **« Unknown users »** : désigne tout utilisateur inconnu ou non authentifié. **NOTE** Pour que les utilisateurs non authentifiés soient automatiquement redirigés vers le portail captif, il faut définir au moins une règle qui s'applique à l'objet

	« **unknown users »**. Cette règle s'appliquera également dès qu'une authentification expire.
Machines sources	La règle s'appliquera à l'objet ou l'utilisateur (créé préalablement au sein de leur menu dédié : `Objets`\module `Objets réseaux` ou `Utilisateurs`\module `Utilisateurs`) que vous sélectionnerez dans ce champ. La machine source est la machine d'où provient la connexion. Vous pouvez **Ajouter** ou **Supprimer** un ou plusieurs objets en cliquant sur l'icône ✚
Interface d'entrée	Interface sur laquelle s'applique la règle de filtrage présentée sous forme de liste déroulante. Par défaut, le firewall la sélectionne automatiquement en fonction de l'opération et des adresses IP source. Il est possible de la modifier pour appliquer la règle sur une autre interface. Cela permet également de spécifier une interface particulière si « Any » a été sélectionnée comme machine source.

Cliquer sur **Ok** pour valider votre configuration.

Onglet « Configuration avancée

Configuration avancée

Port source	Ce champ permet de préciser le port utilisé par la machine source, si c'est une valeur particulière. Par défaut, le module "Stateful" mémorise le port source utilisé et seul celui-ci est autorisé pour les paquets retour.
Via	**Ne pas vérifier** : Cette option implique qu'aucun des deux services suivants ne seront utilisés : la connexion ne passera pas par le proxy HTTP, ne sera pas redirigé vers la page d'authentification et ne passera pas par un tunnel VPN IPsec. **Proxy HTTP explicite** : Le trafic provient du proxy HTTP. **Proxy SSL** : Le trafic provient du proxy SSL. **Tunnel VPN IPsec** : Le trafic provient d'un tunnel VPN IPsec.
DSCP source	Ce champ permet de filtrer en fonction de la valeur du champ DSCP du paquet reçu.

Cliquer sur **Ok** pour valider votre configuration.

Destination

Objet destination utilisé comme critère de sélection pour la règle, un double-clic sur cette zone permettra de choisir la valeur associée dans une fenêtre dédiée.
Celle-ci comporte deux onglets :

Onglet « Général »

Général

Machines destinations	Sélectionnez dans la base objets figurant dans la liste déroulante, la machine destinataire du trafic. Vous pouvez **Ajouter** ou **Supprimer** un objet en cliquant sur l'icône ✚

Cliquer sur **Ok** pour valider votre configuration.

Onglet « Configuration avancée »

Configuration avancée	
Interface de sortie	Cette option permet de choisir l'interface de sortie du paquet sur laquelle s'applique la règle de filtrage. Par défaut, le firewall la sélectionne automatiquement en fonction de l'opération et des adresses IP de destination. Il est possible de filtrer en fonction de l'interface de sortie du paquet.
NAT sur la destination	
Destination	Si vous souhaitez translater l'adresse IP de destination du trafic, sélectionnez en une parmi les objets de la liste déroulante. Sinon, laissez le champ tel qu'il est : à savoir « **None** » par défaut.
Port destination	Si vous souhaitez translater le port de destination du trafic, sélectionnez en un parmi les objets de la liste déroulante. Sinon, laissez le champ tel qu'il est : à savoir « **None** » par défaut.

Cliquer sur **Ok** pour valider votre configuration.

Port dest.

Le port de destination représente le port sur lequel la machine « source » ouvre une connexion sur une machine de «destination ».
Il faut le définir dans la fenêtre d'édition du protocole.

Protocole

Ce champ désigne le protocole sur lequel s'applique la règle de filtrage.

Port

Port destination	Service ou groupe de service utilisé comme critère de sélection pour cette règle. Un double-clic sur cette zone permet de choisir l'objet associé. **Exemples:** Port 80 : service HTTP Port 25 : service SMTP Vous pouvez **Ajouter** ou **Supprimer** un ou plusieurs objets en cliquant sur l'icône ✚ .

Type de protocole

Selon le type de protocole que vous choisissez ici, le champ qui suivra s'affichera différemment :

Détection automatique du protocole (par défaut)	Si vous cochez cette option, un champ du même nom apparaîtra en dessous avec les données suivantes : Protocole applicatif : Auto Protocole IP : Tous
Protocole applicatif	Lorsque vous cochez cette case, le champ suivant portant le même nom vous propose de choisir : Protocole applicatif : Choisissez le protocole souhaité dans la liste déroulante. Protocole IP : Tous
Protocole IP	Si vous cochez cette option, le champ suivant proposera une liste déroulante de différents protocoles IP.

Port translaté

Port destination translaté	Port vers lequel est faite la translation. Les paquets réseaux reçus seront redirigés sur un port donné d'une machine ou un équipement réseau vers une autre machine ou équipement réseau.

Inspection de sécurité

Type d'inspection

Général

Niveau d'inspection

IPS (Détecter et bloquer)	Si vous sélectionnez cette option, l'IPS NETASQ (*Intrusion Prevention System*) détectera et bloquera les tentatives d'intrusion de la couche « réseau » à la couche « applicative » du modèle OSI.
IDS (Détecter)	En sélectionnant cette option, l'IDS NETASQ (*Intrusion Detection System*) détectera les tentatives d'intrusion sur votre trafic, mais sans les bloquer.
Firewall (Ne pas inspecter)	Cette option ne donne accès qu'aux fonctions de base de sécurité informatique, et ne fera que filtrer votre trafic sans l'inspecter.

Configuration

Auto, Config 00 à 09 [par défaut]	Vous pouvez personnaliser la configuration de votre inspection de sécurité en lui attribuant une politique prédéfinie, celle-ci apparaîtra dans la grille de filtrage. Les configurations numérotées peuvent être renommées dans le menu `Protection applicative\Profils d'inspection`.

Inspection applicative

Antivirus	Les boutons **On**/ **Off** vous permettent d'activer ou de désactiver l'Antivirus au sein de votre règle de filtrage.
Antispam	Les boutons **On**/ **Off** vous permettent d'activer ou de désactiver l'Antispam au sein de votre règle de filtrage.
Filtrage URL	Choisissez une politique de filtrage URL au sein des politiques proposées. Vous pouvez choisir de l'activer ou non (boutons **On**/ **Off**).
Filtrage SMTP	Choisissez une politique de filtrage SMTP au sein des politiques proposées. Vous pouvez choisir de l'activer ou non (boutons **On**/ **Off**). **NOTE** Le choix d'une politique de filtrage SMTP active également le proxy POP3 dans le cas où la règle de filtrage autorise le protocole POP3.
Filtrage FTP	Les boutons **On**/ **Off** vous permettent d'activer ou de désactiver le Filtrage FTP au sein de votre règle de filtrage.
Filtrage SSL	Choisissez une politique de filtrage SSL au sein des politiques proposées. Vous pouvez choisir de l'activer ou non (boutons **On**/ **Off**).

Commentaire

Vous pouvez ajouter une description permettant de distinguer plus facilement votre règle de filtrage et ses caractéristiques.

Vérification en temps réel de la politique

La politique de filtrage d’un firewall est un des éléments les plus importants pour la protection de vos données ou de vos ressources internes. Bien que cette politique évolue sans cesse, s’adapte aux nouveaux services, aux nouvelles menaces, aux nouvelles demandes des utilisateurs, elle doit conserver une cohérence parfaite afin que des failles n’apparaissent pas dans la protection que propose le firewall.

L’enjeu est d’éviter la création de règles qui en inhiberait une autre. Lorsque la politique de filtrage est conséquente, le travail de l’administrateur est d’autant plus fastidieux que ce risque s’accroît. De plus lors de la configuration avancée de certaines règles de filtrage très spécifiques, la multiplication des options pourrait entraîner la création d’une règle erronée, ne correspondant plus aux besoins de l’administrateur.

Pour éviter cela, l’écran d’édition des règles de filtrage des firewalls dispose d’un champ de « **Vérification de la politique** » (situé en dessous de la grille de filtrage), qui prévient l’administrateur en cas d’inhibition d’une règle par une autre ou d’erreur sur une des règles qui a été créées.

Exemple
Si vous laisser « **passer** » tout type de trafic (« **Any** ») en règle 1, toute tentative de blocage au sein de la règle 2 sera refusée.

Le message suivant s’affichera :

 *[Règle 2] Cette règle ne sera jamais appliquée car elle est couverte par la règle 1.*

L’onglet « NAT »

Le NAT (*Network Adress Translation)* ou la translation d’adresses a pour principe de convertir une adresse IP en une autre lors du passage par le firewall, quelle que soit la provenance de la connexion. Il est également possible par son biais de faire de la translation de ports.

NOTE GENERALE :
Chaque fois que vous rencontrerez une liste déroulante d’objets au sein des colonnes (exceptées « Etat » et « Action **»**) une icône d’opérateur de comparaison mathématiques apparaîtra ( ). Elle ne sera utilisable que si un autre objet que « **Any** » est sélectionné.

Vous pourrez ainsi personnaliser les paramètres de votre trafic par le biais de l’icône suivante de 4 manières différentes :

- « = » (ou): la valeur de l’attribut correspond à ce qui est sélectionné.
- « != » (ou) la valeur de l’attribut est différente de ce qui est sélectionné.
- « < » (ou ; utilisable pour les ports source et destination uniquement) : le numéro de port du trafic est inférieur à ce qui est sélectionné.
- « > » (ou ; utilisable pour les ports source et destination uniquement) : le numéro du port du trafic est supérieur à ce qui est sélectionné.

A partir de la version 9.0.1, si vous cliquez rapidement 10 fois sur le bouton "Monter", vous distinguez la règle monter visuellement mais la fenêtre d'attente n'apparaît que lorsqu'on ne touche plus au bouton au-delà de 2 ou 3 secondes. Et au final, une seule commande sera passée.

 **NOTE**
Ceci rend le déplacement des règles beaucoup plus fluide.

Les actions sur les règles de la politique de NAT

Rechercher	Ce champ permet la recherche par occurrence, lettre ou mot. **Exemple :** Si vous saisissez « Any » dans le champ, toutes les règles de NAT comportant « Any » s'afficheront dans la grille.
Nouvelle règle	Insérer une ligne à configurer après la ligne sélectionnée, 3 choix sont possibles : • **Règle standard** : Cette option permet de créer une règle de base, en remplissant les différents champs de la grille de NAT. • **Séparateur-regroupement de règles** : Cette option permet d'insérer un séparateur au dessus de la règle sélectionnée afin d'indiquer un commentaire sur une ligne d'édition du NAT, par exemple. Le but de cette option est de regrouper les règles jusqu'au prochain séparateur. Vous pouvez plier et déplier le nœud du séparateur afin de masquer ou afficher le regroupement de règle. • **Règle de NAT statique :** Le principe de la translation d'adresse statique est de convertir une adresse IP (ou N adresses IP, ou adresse publique par exemple) en une autre (ou en N adresses IP privée, par exemple) lors du passage par le firewall, quelle que soit la provenance de la connexion. Une fenêtre d'assistant vous permet d'associer une IP privée et une IP publique (virtuelle) en définissant leurs paramètres. Vous devez choisir au sein des listes déroulantes, les **Machines privées** et **virtuelles** pour vos IP, ainsi que l'interface sur laquelle vous souhaitez les appliquer. Le champ de **Configuration avancée** permet de restreindre l'application à un port ou un groupe de ports, ainsi que d'activer la Publication ARP. Cette dernière permet de rendre disponible l'IP à publier via l'adresse MAC du firewall. Cliquez ensuite sur **Terminer** pour valider votre configuration.  **NOTE** Pour une règle de translation bidirectionnelle (bimap) de N vers N, les plages d'adresses, réseaux ou groupes de machines originaux et translatés doivent être de même taille. La translation bidirectionnelle est généralement utilisée pour donner accès à un serveur depuis l'extérieur avec une adresse IP publique qui n'est pas l'adresse réelle de la machine. Les plages d'adresses sont supportées par l'action bidirectionnelle. Les adresses sources et translatées sont utilisées dans l'ordre : la plus "petite" adresse du champ source est translatée vers la plus "petite" adresse du champ translaté.
Supprimer	Ce champ permet de supprimer la ligne sélectionnée.  **NOTE** Il est possible de supprimer plusieurs lignes en même temps, en les sélectionnant avec la touche « Ctrl » puis en cliquant sur **Supprimer**.
Monter	Placer la ligne sélectionnée avant la ligne directement au dessus.
Descendre	Placer la ligne sélectionnée après la ligne directement en dessous.
Réinit. colonnes	Lorsque vous cliquez sur la flèche de droite dans le champ du nom d'une colonne (exemple : **Etat**), vous avez la possibilité d'afficher des colonnes supplémentaires ou d'en retirer afin qu'elles ne soient pas visibles à l'écran, grâce à un système de coche. **Exemple** : Vous pouvez cocher les cases « **Nom** » et « **Port src** » qui ne sont pas affichées par défaut.

En cliquant que le bouton **réinit. colonnes**, vos colonnes réapparaîtront à l’état initial, avant que vous n’ayez coché de case additionnelle. Ainsi, les cases « **Nom** » et « **Port src** » seront de nouveau masquées.

La grille de NAT

La grille du NAT est divisée en deux : elle comporte d’une part, le **Trafic original (avant translation)**, et d’autre part, le **Trafic translaté.**

Etat Etat de la règle :

Activé, la règle est activée et sera utilisée par le firewall NETASQ.

Désactivé, la règle est désactivée : double-cliquez dans le champ pour activer ou désactiver la règle.


REMARQUE

Le firewall va évaluer les règles dans leur ordre d’apparition à l’écran : une à une en partant du haut. Dés qu'il rencontre une règle qui correspond à la demande, il effectue l'action spécifiée et s’arrête là.

A partir de la version 9.0.1, la translation d’adresse source gère les protocoles IP sans état (type GRE) toutefois avec la limitation suivante :
Si deux clients passent par le même firewall, ils ne pourront pas se connecter sur un même serveur en même temps.
Le moteur de prévention d’intrusion NETASQ va bloquer les paquets reçus par le second client.
Au bout de 5 minutes, le moteur de prévention d’intrusion jugera la session trop ancienne et permettra au second client de prendre le relai.

Le trafic original (avant translation)

En cliquant dans la colonne « Interface d’entrée » une fenêtre de configuration s’affiche :

Source du trafic (avant translation)

Onglet « Général »
Général

Utilisateurs	La règle s’appliquera à l’utilisateur que vous sélectionnerez dans ce champ. Il en existe trois par défaut : **« No user » :** Cette option permet de vider le champ utilisateur et de ne plus y appliquer de critère pour la règle. **« Any user »** : désigne tout utilisateur authentifié. **« Unknown users »** : désigne tout utilisateur inconnu ou non authentifié.
Machines sources	La règle s’appliquera à l’objet que vous sélectionnerez dans ce champ. La machine source est la machine d’où provient le paquet traité : elle est l’émetteur du paquet. **NOTE** Plusieurs objets peuvent être spécifiés en même temps.
Interface d’entrée	Interface sur laquelle s’applique la règle de translation présentée sous forme de liste déroulante. Par défaut, le firewall la sélectionne automatiquement en fonction de l'opération et des adresses IP source et destination. Il est possible de la modifier pour appliquer la règle sur une autre interface.

Cliquer sur **Ok** pour valider votre configuration.

Onglet « Configuration avancée »
Configuration avancée

Port source	Ce champ permet de préciser le port source utilisé par la machine source. Par défaut, le mode « Stateful » mémorise le port source utilisé et seul celui-ci est autorisé pour les paquets retour.
DSCP source	Ce champ désigne le code DSCP source du paquet reçu.

Cliquer sur **Ok** pour valider votre configuration.
Il faut ensuite définir l'interface de sortie du trafic :

Destination du trafic (avant translation)

Onglet « Général »
Général

Machines destinations	Sélectionnez dans la base objets figurant dans la liste déroulante, la machine destinataire de votre trafic IP.
Port destination	Si vous souhaitez translater le port de destination du trafic, sélectionnez en un parmi les objets de la liste déroulante. L'objet « Any » est sélectionné par défaut.

A partir de la version 9.0.1, des types d'équilibrages de charge autres que le hachage de connexion peuvent maintenant être sélectionnés avec une plage de ports de destination.
Cliquer sur **Ok** pour valider votre configuration.

Onglet « Configuration avancée »
Configuration avancée

Interface de sortie	Interface depuis laquelle le trafic quitterait le firewall avant translation. Par défaut, le firewall la sélectionne automatiquement en fonction de l'opération et des adresses IP source et destination. Il est possible de la modifier pour restreindre la règle à une interface.

Le trafic après translation

Source du trafic après translation

Onglet « Général »

Machine source translatée	La règle s'appliquera à l'objet que vous sélectionnerez dans ce champ. La machine source translatée fait référence à la nouvelle adresse IP de la machine source, après sa translation par opération de NAT.
Port source translaté.	Ce champ permet de préciser le port source utilisé par la machine source après la translation. Par défaut, le mode "Stateful" mémorise le port source utilisé et seul celui-ci est autorisé pour les paquets retour.
Choisir aléatoirement le port source translaté	En cochant cette option, le firewall va sélectionner de manière aléatoire le port source translaté dans la liste.

Cliquer sur **Ok** pour valider votre configuration.

Onglet « Configuration avancée »

Répartition de charge	Cette option permet de répartir les adresses IP sources d'émission du paquet après translation. La méthode de répartition de charge dépend de l'algorithme utilisé. Plusieurs algorithmes de répartition de charge sont disponibles : **Aucune** : Aucune répartition de charge ne sera effectuée. **Round-robin** : Cet algorithme permet de répartir équitablement la charge parmi les différentes IP de la plage d'adresses sélectionnée. Chacune de ces adresses IP sources. **Hachage de l'IP source** : Un hash de l'adresse source est effectué pour choisir l'adresse de la plage à utiliser. Cette méthode permet de garantir qu'une adresse source donnée sera toujours associée avec la même adresse de la plage. **Aléatoire** : Le firewall sélectionne aléatoirement une adresse parmi la plage d'adresses sélectionnée
Publication ARP	Cette option permet de rendre disponible l'IP à publier via l'adresse MAC du firewall.

Cliquer sur **Ok** pour valider votre configuration.

Destination du trafic après translation

Onglet « Général »

Machine destination translatée	Ce champ permet de sélectionner la machine destinataire du paquet translaté au sein de la liste déroulante d'objets.
Port destination translaté	Ce champ permet de préciser le port destination utilisé par la machine de destination.

Cliquer sur **Ok** pour valider votre configuration.

Onglet « Configuration avancée »

Répartition de charge	Cette option permet de répartir la transmission de paquet entre plusieurs adresses IP de destination. La méthode de répartition de charge dépend de l'algorithme utilisé. Plusieurs algorithmes de répartition de charge sont disponibles : **Aucune** : Aucune répartition de charge ne sera effectuée. **Round-robin** : Cet algorithme permet de répartir équitablement la charge parmi les différentes IP de la plage d'adresses sélectionnée. Chacune de ces adresses IP sources. **Hachage de l'IP source** : Un hash de l'adresse source est effectué pour choisir l'adresse de la plage à utiliser. Cette méthode permet de garantir qu'une adresse source donnée sera toujours associée avec la même adresse de la plage. **Aléatoire** : Le firewall sélectionne aléatoirement une adresse parmi la plage d'adresses sélectionnée
Publication ARP	Cette option permet de rendre disponible l'IP à publier via l'adresse MAC du firewall.

Cliquer sur **Ok** pour valider votre configuration.

Commentaire

Vous pouvez ajouter une description permettant d'affiner votre règle de NAT et ses caractéristiques.

Exemple de règle de NAT

Trafic original (avant translation)			Trafic après translation
Source	Destination	Port dest	Destination
Internet sur on	**Virtual_mail server**	**smtp**	**Internal_mail serveur ARP**

Vérification en temps réel de la politique

La politique de NAT d'un firewall est un des éléments les plus importants pour la sécurité des ressources que le firewall protège. Bien que cette politique évolue sans cesse, s'adapte aux nouveaux services, aux nouvelles menaces, aux nouvelles demandes des utilisateurs, elle doit converser une cohérence parfaite afin que des failles n'apparaissent pas dans la protection que propose le firewall.

L'enjeu est d'éviter la création de règles qui en inhiberaient d'autres. Lorsque la politique de filtrage est conséquente, le travail de l'administrateur est d'autant plus fastidieux que ce risque s'accroît. De plus lors de la configuration avancée de certaines règles de filtrage très spécifiques, la multiplication des options pourrait entraîner la création d'une règle erronée, ne correspondant plus aux besoins de l'administrateur.

Pour éviter cela, l'écran d'édition des règles de filtrage des firewalls dispose d'un champ de « **Vérification de la politique** » (situé en dessous de la grille de filtrage), qui prévient l'administrateur en cas d'inhibition d'une règle par une autre ou d'erreur sur une des règles qui a été créées.

Exemple
Si vous laisser « **passer** » tout type de trafic (« **Any** ») en règle 1, toute tentative de blocage au sein de la règle 2 sera refusée.

Le message suivant s'affichera :

[Règle 2] Cette règle ne sera jamais appliquée car elle est couverte par la règle 1.

FILTRAGE SMTP

Ce module se compose de 2 zones :
- Une zone destinée aux profils,
- Une zone destinée aux règles de filtrage SMTP.

Les profils

Le bandeau vous permet de manipuler les profils associés au filtrage SMTP.

Sélection du profil

Le menu déroulant propose 10 profils, numérotés de 00 à 09.
Chaque profil possède par défaut, le nom « Default », accompagné de sa numérotation.
Exemples :
- (0) Defaut00
- (1) Default01…

Pour sélectionner un profil, il faut cliquer sur la flèche à droit du champ dans lequel est inscrit par défaut « Default00 », et choisir le profil voulu.

Par défaut, chaque profil est configuré de la manière suivante :

Etat	Action	Expéditeur	Destinataire (to,cc,cci)	Commentaire
Activé	Passer	*@*	*@*	default rule (pass all)

Les boutons

Editer	Cette fonction permet d'effectuer 3 actions sur les profils : - **Renommer** : en cliquant sur cette option, une fenêtre composée de deux champs à remplir s'affiche. Celle-ci propose de modifier le nom d'une part et d'ajouter un commentaire d'autre part. Une fois l'opération effectuée, cliquez sur « Mis à jour ». Il est également possible d' « annuler » la manipulation. - **Réinitialiser** : Permet de rendre au profil sa configuration initiale, de sorte que toutes les modifications apportées soient supprimées. - **Copier vers** : Cette option permet de copier un profil vers un autre, toutes les informations du profil copié seront transmises au profil récepteur. Il portera également le même nom.
Dernière modification	Cette icône permet de connaître la date et l'heure exactes de la dernière modification effectuée. Un commentaire peut également être ajouté.

Les règles

Référez-vous à la procédure suivante pour éditer un profil de filtrage SMTP :

1. Sélectionnez un profil dans la liste des profils de filtrage d'URL.
2. La grille de filtrage se présente ainsi qu'un écran d'indication d'erreur.

Les manipulations possibles

Bouton **Ajouter** : Insérer une ligne vierge après la ligne sélectionnée.
Bouton **Supprimer** : Supprimer la ligne sélectionnée.
Bouton **Monter** : Placer la ligne sélectionnée avant la ligne directement au dessus.
Bouton **Descendre** : Placer la ligne sélectionnée après la ligne directement en dessous.

La grille

La grille présente les colonnes suivantes :

Etat	Etat de la règle : **Activé**, la règle est utilisée pour le filtrage. **Désactivé**, la règle n'est pas utilisée pour le filtrage. Lorsque la règle est désactivée, la ligne est grisée afin de refléter la désactivation. **REMARQUE** Le firewall va évaluer les règles dans leur ordre d'apparition à l'écran : une à une en partant du haut. Dés qu'il rencontre une règle qui correspond à la demande, il effectue l'action spécifiée et s'arrête là. Ce qui signifie que, si l'action spécifiée au sein de la règle correspond à **Bloquer**, toutes les règles effectuées en dessous de celle-ci passeront automatiquement en **Bloquer** également.
Action	Permet de spécifier le résultat de la règle : **Passer** pour autoriser l'envoi et la réception des mails, **Bloquer** pour les interdire
Expéditeur	Définition de l'émetteur du mail. ***A partir de la version 9.0.1,*** la sélection de « none » en tant qu'expéditeur est possible.
Destinataire (to, cc, cci)	Définition du destinataire du mail.
Commentaire	Commentaire associé à la règle.

La saisie d'un masque d'e-mails peut comporter la syntaxe suivante :

- * : remplace une séquence de caractères quelconque.

Exemple

*@netasq.com permet de définir l'ensemble des emails domaine Internet de la société NETASQ.

Il est également possible de trouver :

- ? : pour le remplacement d'un caractère
- <vide> : Cette valeur ne peut être obtenue que lorsque le champ **Expéditeur** est vide. Elle n'est utilisée que pour le cas des "Mailer Deamon".En effet, lorsqu'un mail ne trouve pas de destinataire sur le serveur mail distant, un message d'erreur est renvoyé par le serveur mail distant, indiquant qu'il y a erreur sur le destinataire. Dans ce cas, le champ **Expéditeur** de ce message d'erreur est vide.

  Il est possible de créer une règle avec l'action « bloquer » qui empêchera l'envoi de mail si l'expéditeur n'est pas connu.

Erreurs trouvées dans la politique de filtrage SMTP

L'écran d'édition des règles de filtrage SMTP des firewalls dispose d'un analyseur de cohérence et de conformité des règles qui prévient l'administrateur en cas d'inhibition d'une règle par une autre ou d'erreur sur une des règles qui a été créées.
Cet analyseur regroupe les erreurs de création de règles et les erreurs de cohérence.
Les erreurs sont présentées sous forme de liste. En cliquant sur une erreur, la règle concernée sera automatiquement sélectionnée.

FILTRAGE SSL

Le filtrage SSL est désormais intégré à la nouvelle politique de sécurité des firewalls multifonctions NETASQ. Ce module permet de filtrer l'accès aux sites web sécurisés. Il rend possible l'autorisation et l'interdiction des sites web ou des certificats comportant des risques.

Ce module se compose de 2 zones :

- Une zone destinée aux profils,
- Une zone destinée aux règles de filtrage SSL.

Les profils

Le bandeau vous permet de manipuler les profils associés au filtrage SSL.

Sélection du profil

Le menu déroulant propose 10 profils, numérotés de 00 à 09.
Chaque profil possède par défaut, le nom « Default », accompagné de sa numérotation.
Exemples :

- (0) Defaut00
- (1) Default01…

Pour sélectionner un profil, il faut cliquer sur la flèche à droit du champ dans lequel est inscrit par défaut « Default00 », et choisir le profil voulu.

Par défaut, chaque profil est configuré de la manière suivante :

Etat	Action	URL-CN	Commentaire
Activé	Passer sans déchiffrer	any	default rule (decrypt all)

Les boutons

Editer	Cette fonction permet d'effectuer 3 actions sur les profils : • **Renommer** : en cliquant sur cette option, une fenêtre composée de deux champs à remplir s'affiche. Celle-ci propose de modifier le nom d'une part et d'ajouter un commentaire d'autre part. Une fois l'opération effectuée, cliquez sur « Mis à jour ». Il est également possible d' « annuler » la manipulation. • **Réinitialiser** : Permet de rendre au profil sa configuration initiale, de sorte que toutes les modifications apportées soient supprimées. • **Copier vers** : Cette option permet de copier un profil vers un autre, toutes les informations du profil copié seront transmises au profil récepteur. Il portera également le même nom.
Dernière modification	Cette icône permet de connaître la date et l'heure exactes de la dernière modification effectuée. Un commentaire peut également être ajouté.

Les règles

Référez-vous à la procédure suivante pour éditer un profil de filtrage SSL :

1 Sélectionnez un profil dans la liste des profils de filtrage SSL.

2 La grille de filtrage se présente ainsi qu'un écran d'indication d'erreur.

Les manipulations possibles

Bouton **Ajouter** : Insérer une ligne à configurer après la ligne sélectionnée.
Bouton **Supprimer** : Supprimer la ligne sélectionnée.
Bouton **Monter** : Placer la ligne sélectionnée avant la ligne directement au dessus.
Bouton **Descendre** : Placer la ligne sélectionnée après la ligne directement en dessous.

La grille

La grille présente les colonnes suivantes :

Etat	Etat de la règle : **Activé**, la règle est utilisée pour le filtrage. **Désactivé**, la règle n'est pas utilisée pour le filtrage. Lorsque la règle est désactivée, la ligne est grisée afin de refléter la désactivation. **REMARQUE** Le firewall va évaluer les règles dans leur ordre d'apparition à l'écran : une à une en partant du haut. Dés qu'il rencontre une règle qui correspond à la demande, il effectue l'action spécifiée et s'arrête là. Ce qui signifie que, si l'action spécifiée au sein de la règle correspond à **Bloquer**, toutes les règles effectuées en dessous de celle-ci seront considérées **Bloquer** également.
Action	Permet de spécifier l'opération à effectuer : Si **Passer sans déchiffrer** spécifié, l'accès au CN demandé est autorisé sans analyse SSL préalable. Si **Bloquer sans déchiffrer** est spécifié, l'accès au CN demandé est refusé, sans qu'aucune analyse SSL ne soit effectuée. La connexion est coupée. Si **Déchiffrer** est spécifié, l'analyse protocolaire sera appliquée sur le flux déchiffré, ainsi que sur un proxy, si une règle est créée pour cela.
URL-CN	L'action s'applique en fonction de la valeur de cette colonne, elle peut contenir un groupe ou une catégorie d'URL, ainsi qu'un groupe de noms de certificats.
Commentaire	Commentaire associé à la règle.

Erreurs trouvées dans la politique de filtrage SSL

L'écran d'édition des règles de filtrage SSL des firewalls dispose d'un analyseur de cohérence et de conformité des règles qui prévient l'administrateur en cas d'inhibition d'une règle par une autre ou d'erreur sur une des règles qui a été créées.
Cet analyseur regroupe les erreurs de création de règles et les erreurs de cohérence.
Les erreurs sont présentées sous forme de liste. En cliquant sur une erreur, la règle concernée sera automatiquement sélectionnée.

FILTRAGE URL

Ce module se compose de 2 zones :

- Une zone destinée aux profils,
- Une zone destinée aux règles de filtrage d'URL.

Les profils

Le bandeau vous permet de manipuler les profils associés au filtrage URL.

Sélection du profil

Le menu déroulant propose 10 profils, numérotés de 00 à 09.
Chaque profil possède par défaut, le nom « Default », accompagné de sa numérotation.
Exemples :

- (0) Defaut00
- (1) Default01…

Pour sélectionner un profil, il faut cliquer sur la flèche à droit du champ dans lequel est inscrit par défaut « Default00 », et choisir le profil voulu.
Par défaut, chaque profil est configuré de la manière suivante :

Etat	Action	Groupe d'URL	Commentaire
Activé	Passer	any	default rule (pass all)

Les boutons

Editer	Cette fonction permet d'effectuer 3 actions sur les profils : • **Renommer** : en cliquant sur cette option, une fenêtre composée de deux champs à remplir s'affiche. Celle-ci propose de modifier le nom d'une part et d'ajouter un commentaire d'autre part. Une fois l'opération effectuée, cliquez sur « Mis à jour ». Il est également possible d' « annuler » la manipulation. • **Réinitialiser** : Permet de rendre au profil sa configuration initiale, de sorte que toutes les modifications apportées soient supprimées. Le profil redevient « actif » sous l'action **Passer**, appliquée à tous les groupes d'URL. • **Copier vers** : Cette option permet de copier un profil vers un autre, toutes les informations du profil copié seront transmises au profil récepteur. Il portera également le même nom.
Dernière modification	Cette icône permet de connaître la date et l'heure exactes de la dernière modification effectuée. Un commentaire peut également être ajouté.

Les règles

Référez-vous à la procédure suivante pour éditer un profil de filtrage d'URL :

1 Sélectionnez un profil dans la liste des profils de filtrage d'URL.

2 La grille de filtrage se présente ainsi qu'un écran d'indication d'erreur.

Les manipulations possibles

Bouton **Ajouter** : Insérer une ligne à configurer après la ligne sélectionnée.
Bouton **Supprimer** : Supprimer la ligne sélectionnée.
Bouton **Monter** : Placer la ligne sélectionnée avant la ligne directement au dessus.
Bouton **Descendre** : Placer la ligne sélectionnée après la ligne directement en dessous.

La grille

La grille présente les colonnes suivantes :

Etat	Etat de la règle : **Activé**, la règle sera active lorsque cette politique de filtrage sera sélectionnée. **Désactivé**, la règle ne sera pas opérationnelle. La ligne sera grisée afin de refléter la désactivation.  **REMARQUE** Le firewall va évaluer les règles dans leur ordre d'apparition à l'écran : une à une en partant du haut. Dés qu'il rencontre une règle qui correspond à la demande, il effectue l'action spécifiée et s'arrête là. Ce qui signifie que, si l'action spécifiée au sein de la règle correspond à **Bloquer**, toutes les règles effectuées en dessous de celle-ci passeront automatiquement en **Bloquer** également.
Groupe d'URL	Un nom de groupe d'URL précédemment créé. En cliquant sur le champ, une liste déroulante vous invite à choisir un groupe d'URL, issu de la base objets. Le groupe <Any> correspond à n'importe quelle URL, même si elle ne fait pas partie des groupes d'URL.
Action	Permet de spécifier le résultat de la règle, **Passer** pour autoriser le site, **Bloquer** pour interdire l'accès et clore directement la connexion sans message de blocage, **Rediriger vers la page de blocage** pour interdire l'accès et afficher la page de blocage.
Commentaire	Commentaire associé à la règle.

 **REMARQUE**
Le cliquer-glisser (dran'n'drop) ne s'applique ici que pour les groupes d'URL.

A partir de la version 9.0.1, les caractères « [ ] » et « {} » ne sont plus autorisés dans les URL (Internet Explorer 7 et 8).

Erreurs détectées

L'écran d'édition des règles de filtrage d'URL des firewalls dispose d'un analyseur de cohérence et de conformité des règles qui prévient l'administrateur en cas d'inhibition d'une règle par une autre ou d'erreur sur une des règles qui a été créées.
Cet analyseur regroupe les erreurs de création de règles et les erreurs de cohérence.
Les erreurs sont présentées sous forme de liste. En cliquant sur une erreur, la règle concernée sera automatiquement sélectionnée.

HAUTE DISPONIBILITE

Ce module va vous permettre dans un premier temps, de créer un cluster ou groupe de firewalls. Une fois ceci fait, un autre firewall pourra rejoindre celui que vous venez d'initialiser.
La Haute Disponibilité NETASQ fonctionne sur le mode « Actif/passif » : un cluster contenant 2 firewalls, si celui considéré comme « actif » tombe, ou qu'un câble est débranché, le second firewall, considéré comme « passif » prend le relai de manière transparente. Ainsi, le firewall « passif » devient « actif ».

La configuration de la Haute Disponibilité se déroule en 4 étapes.

- Etape 1 : Créer un groupe de firewalls (cluster)/rejoindre un groupe de firewalls (cluster) existant
- Etape 2 : Configuration des interfaces réseaux : le lien principal et le lien secondaire (facultatif)
- Etape 3 : Définition de la clé pré partagée du cluster
- Etape 4 : Résumé des étapes et application des paramètres configurés

Une fois ces 4 étapes terminées, un nouvel écran s'affichera vous proposant d'effectuer de nouvelles configurations au sein de la HA.

Etape 1 : Créer ou rejoindre un cluster en Haute Disponibilité

Créer un groupe de firewalls (cluster)	Lorsque vous cochez cette option, le boîtier se tient prêt à recevoir les autres firewalls et s'ajoute lui-même au cluster.
Rejoindre un groupe de firewalls (cluster)	Lorsque vous cochez cette option, le boîtier va tenter de se connecter à celui renseigné par l'adresse IP définie lors de la création du cluster. Ainsi, ce second firewall va récupérer les infos du premier et se synchroniser à lui. Le cluster est ainsi composé de deux firewalls : si le premier tombe, le second prendra le relai de manière transparente.  NOTE Un reboot sera effectué à la fin de l'assistant. Une fois le reboot effectué, le boîtier fait partie du cluster, donc n'existe plus en tant qu'entité, mais en tant que membre du cluster.  AVERTISSEMENT Lorsque vous choisissez de « rejoindre » un cluster, il implique que vous en ayez déjà créé un au préalable, en ayant coché l'autre option « **Créer un groupe de firewalls (cluster)** » et en ayant effectué les configurations nécessaires pour sa mise en place sur un premier firewall.

 AVERTISSEMENT

Il est important de ne pas "créer" deux fois de cluster, au quel cas, vous mettriez en place deux clusters HA contenant chacun un firewall, et non un cluster HA contenant 2 firewalls.

Etape 2 : Configuration des interfaces réseaux

Si vous avez choisi de créer un cluster

Lien principal

Interface	Interface principale utilisée pour relier les deux firewalls constituant le cluster. Sélectionnez-là parmi les objets figurant au sein de la liste déroulante.
Définir l'adresse IP	Entrez l'adresse IP à laquelle votre groupe de firewalls (cluster) devra se connecter pour fonctionner.
Définir le masque réseau	Entrez le masque réseau pour votre groupe de firewalls (cluster).

Lien secondaire (facultatif)

Si le firewall ne reçoit pas de réponse sur le lien principal, il va tenter de se connecter à ce lien secondaire. Cela évite que les deux firewalls passent en mode actif/actif si un problème survient sur le lien principal.

Utiliser un second lien de communication	Cochez cette option afin de dégriser les champs du dessous et de définir un lien secondaire pour votre cluster.
Interface	Interface secondaire utilisée pour relier les deux firewalls constituant le cluster. Sélectionnez-là parmi les objets figurant au sein de la liste déroulante.
Définir l'adresse IP	Entrez l'adresse IP pour votre lien secondaire.
Définir le masque réseau	Entrez le masque réseau pour votre lien secondaire.

 **NOTE**

Pour qu'un lien fonctionne, les 2 membres du cluster doivent utiliser la même interface.

Si vous avez choisi de rejoindre un cluster

Cette option sous-entend d'un groupe de firewalls ait déjà été créé au préalable, pour que celui-ci puisse le « rejoindre ».
Ainsi, une partie des informations du premier firewall créé seront reprises.

Lien principal

Interface	Interface principale utilisée pour relier les deux firewalls constituant le cluster. Cette interface doit être la même que celle sélectionnée lors de la création du cluster sur le premier firewall.
Définir l'adresse IP	Adresse IP à laquelle votre groupe de firewalls (cluster) devra se connecter pour fonctionner. Cette adresse doit appartenir au même sous-réseau que celui défini lors de la création du cluster sur le premier firewall.

Définir le masque réseau	Masque réseau pour votre groupe de firewalls (cluster). Ce masque doit être le même que celui utilisé lors de la création du cluster sur le premier firewall

Lien secondaire (facultatif)

Si le firewall ne reçoit pas de réponse sur le lien principal, il va tenter de se connecter à ce lien secondaire. Cela évite que les deux firewalls passent en mode actif/actif si un problème survient sur le lien principal.

Utiliser un second lien de communication	Cochez cette option afin de dégriser les champs du dessous et de définir un lien secondaire pour votre cluster. Cette option ne doit être sélectionnée que si elle l'avait été lors de la création du cluster sur le premier firewall.
Interface	Interface secondaire utilisée pour relier les deux firewalls constituant le cluster. Cette interface doit être la même que celle sélectionnée lors de la création du cluster sur le premier firewall.
Définir l'adresse IP	Adresse IP pour votre lien secondaire. Cette adresse doit appartenir au même sous-réseau que celui défini lors de la création du cluster sur le premier firewall.
Définir le masque réseau	Masque réseau pour votre lien secondaire. Ce masque doit être le même que celui utilisé lors de la création du cluster sur le premier firewall.


NOTE

Pour qu'un lien fonctionne, les 2 membres du cluster doivent utiliser la même interface.

Etape 3 : Clé pré partagée du cluster

En cas de création de cluster

Pour sécuriser la connexion entre les membres du cluster, vous devez définir une clé pré partagée. Celle-ci ne sera utilisée que par les firewalls rejoignant le cluster pour la première fois.

Nouvelle clé pré-partagée	Définissez un mot de passe/une clé pré partagée pour votre cluster.
Confirmer	Confirmation du mot de passe/clé pré partagée, que vous venez de renseigner dans le champ précédent.
Force du mot de passe	Ce champ indique le niveau de sécurité de votre mot de passe : « Très Faible », « Faible », « Moyen », « Bon » ou « Excellent ». Il est fortement conseillé d'utiliser les majuscules et les caractères spéciaux.

Cliquez sur **Suivant**.

En cas de cluster existant

Adresse IP du firewall à contacter	Entrez l'adresse IP que vous avez défini dans l'assistant lors de la création du cluster (adresse IP du lien principal ou secondaire).
Clé pré partagée	Entrez le mot de passe/la clé pré partagée que vous avez défini dans l'assistant lors de la création du cluster. Cette icône  permet d'afficher le mot de passe en clair pour vérifier qu'il n'est pas erroné.

Etape 4 : Résumé et finalisation du cluster

En cas de création de cluster

Après avoir visualisé le résumé de vos configurations, cliquez sur **Terminer**, le message suivant s'affiche :
Ce firewall est prêt à fonctionner en haute disponibilité. Vous pouvez maintenant configurer un autre firewall pour qu'il rejoigne ce cluster.
Votre cluster étant désormais créé, un nouvel écran s'affichera lorsque vous tenterez d'accéder au module.

En cas de cluster existant

Après avoir visualisé le résumé de vos configurations, cliquez sur **Terminer**, le message suivant s'affiche :
Rejoindre le groupe de firewalls nécessite le redémarrage de ce firewall. Etes-vous sûr de vouloir rejoindre le cluster ?
Pour finaliser la configuration, ce firewall va rejoindre le cluster et réaliser la synchronisation de configuration initiale. Il va ensuite redémarrer afin de l'appliquer. Pour accéder au cluster, vous devrez vous connecter au firewall actif.

NOTE

Cette étape peut être longue sur les modèles d'entrée de gamme (U30, U70). Il ne faut pas débrancher le firewall.

Ecran de la Haute disponibilité

Communication entre les firewalls du groupe de haute disponibilité

Lien principal	Interface principale utilisée pour relier les deux firewalls constituant le cluster. Sélectionnez-là parmi les objets figurant au sein de la liste déroulante
Utiliser un second lien de communication	Cochez cette option afin de dégriser les champs du dessous et de définir un lien secondaire pour votre cluster.

Lien secondaire	Interface secondaire utilisée pour relier les deux firewalls constituant le cluster. Sélectionnez parmi les objets figurant au sein de la liste déroulante.



Il est conseillé d'utiliser un lien secondaire lorsque l'on souhaite changer l'interface utilisée en tant que lien principal. En effet, le changement de lien peut provoquer une coupure de la communication entre les membres du cluster, pouvant résulter en un cluster non fonctionnel.

Configuration avancée

Modifier la clé pré partagée entre les firewalls du groupe de haute disponibilité

Nouvelle clé pré partagée	Ce champ permet de modifier la clé pré partagée ou le mot de passe défini lors de la création du cluster.
Confirmer	Confirmation du mot de passe/clé pré partagée, que vous venez de renseigner dans le champ précédent.
Force du mot de passe	Ce champ indique le niveau de sécurité de votre mot de passe : « Très Faible », « Faible », « Moyen », « Bon » ou « Excellent ». Il est fortement conseillé d'utiliser les majuscules et les caractères spéciaux.

Indicateur de qualité

Firewall actif en cas d'égalité

Cette option permet de favoriser un firewall comme actif lorsque les 2 ont le même niveau de qualité. Le but de privilégier un firewall actif est de conserver au maximum les logs sur le même firewall ou de favoriser le trafic sur un firewall spécifique. Si l'actif tombe en panne, ou si un câble se fait débrancher, l'autre passera actif.

Automatique	Si vous choisissez cette option, aucune priorité n'est affectée.
Ce firewall (<son numéro de série>)	En choisissant cette option, vous positionnerez ce firewall comme actif et le second le relayera si celui tombe en panne ou est débranché.
L'autre firewall (distant) (<son numéro de série>)	En choisissant cette option, vous positionnerez ce firewall comme actif et le second le relayera si celui tombe en panne ou est débranché. **AVERTISSEMENT** Le choix de cette option va provoquer un swap immédiat, ou basculement de ce firewall en tant que firewall actif, entraînant une déconnexion de l'interface d'administration.

A partir de la version 9.0.1, Une option a été ajoutée pour accélérer la prise en compte de la bascule d'un cluster en mode bridge par les équipements environnants. Si l'option est active, les interfaces du bridge sont réinitialisées au moment de la bascule pour forcer les commutateurs connectés au firewall à renouveler leur table ARP.

Communication entre les firewalls du groupe de haute disponibilité

Chiffrer la communication entre les firewalls	Par défaut, les communications entre les firewalls ne sont pas chiffrées, partant du principe que le lien utilisé par la HA est un lien dédié. Dans certaines architectures, le lien HA n'est pas dédié, et si on souhaite que les communications inter-cluster soient indéchiffrables, on peut les chiffrer (en AES, par exemple).  **AVERTISSEMENTS** 1) Cocher cette option peut dégrader les performances de votre HA. 2) Seules les connexions passent sur le lien HA et non leurs contenus.

ARP gratuit

Transmettre périodiquement des requêtes ARP gratuites	En cochant cette case, vous enverrez, à intervalles réguliers, des annonces ARP, afin que les différents éléments du réseau (switch, routeurs, …) puissent mettre à jour leurs propres tables ARP.  **NOTE** Lors du passage actif, le firewall enverra tout de même une annonce ARP, indifféremment de cette option
Fréquence (en secondes)	Ce champ permet de définir la fréquence en secondes des requêtes ARP, dans la limite 9999 secondes maximum.

Impact de l'indisponibilité d'une interface dans l'indicateur de qualité d'un firewall

Interface	Cette colonne liste toutes les interfaces Ethernet de votre firewall.
Poids [0-9999]	Le poids permet de donner une valeur relative à l'interface. Le nombre « 100 » a été donné par défaut aux interfaces listées. Elles sont donc toutes d'égale importance. Vous pouvez modifier ce critère en sélectionnant la case voulue. spécifier que l'interface « in » est plus importante que l'interface « out » et les autres interfaces en lui attribuant le nombre 150. **NOTE** Il peut être intéressant de placer les interfaces inutilisées à 0, afin qu'elles n'entrent pas en compte dans le calcul de la qualité.

Cliquez ensuite sur **Appliquer.**

INTERFACES

Le module `Interfaces` permet de gérer, ajouter, supprimer des éléments réseaux appelés "interfaces réseau" qui représentent des éléments physiques ou non de communication entre les différents réseaux qui transitent par le boîtier.

Les bridges se composent de 3 onglets, les interfaces se composent de 2 onglets (ethernet et vlan) et les modems d'1 seul onglet.

Mode de fonctionnement entre interfaces

Vous pouvez configurer le fonctionnement entre interfaces du firewall suivant trois modes différents:

- Mode avancé
- Mode Bridge (ou mode transparent)
- Mode hybride

Mode avancé

En avancé : chaque interface possède une adresse IP différente et le réseau qui lui est relié fait partie de la même classe. Cela permet de configurer des règles de translation pour accéder à une autre zone du firewall.
Avec ce mode de configuration, le firewall fonctionne comme un routeur|tag=gloss_Routeur entre ses différentes interfaces.
Cela implique certains changements d'adresses IP sur les routeurs ou serveurs lorsque vous les déplacez dans un réseau différent (derrière une interface du firewall différente).

Les avantages de ce mode sont :

- La possibilité de faire de la translation d'adresses d'une classe d'adresses vers une autre.
- Seul le trafic passant d'une interface à l'autre traverse le firewall (réseau interne vers Internet par exemple). Cela allège considérablement le firewall et fournit de meilleurs temps de réponse.
- Meilleure distinction des éléments appartenant à chaque zone (interne, externe et DMZ). La distinction se fait par les adresses IP qui sont différentes pour chaque zone. Cela permet d'avoir une vision plus claire des séparations et de la configuration à appliquer pour ces éléments.

Mode Bridge ou mode transparent

En transparent (Bridge) : les interfaces font partie du même plan d'adressage déclaré sur le bridge.
Le mode transparent, aussi appelé "Bridge" en anglais, permet de conserver le même adressage entre les interfaces.
Il simule un pont|tag=gloss_PONT (BRIDGE) filtrant, c'est-à-dire qu'il est traversé par l'ensemble du trafic du réseau.

Cependant, vous pouvez ensuite filtrer les flux qui le traversent, en utilisant les objets interfaces ou les plages d'adresses suivant vos besoins et donc protéger telle ou telle partie du réseau.

Les avantages de ce mode sont multiples :

- Facilité d'intégration du produit car pas de changement de la configuration des postes client (routeur par défaut, routes statiques...) et aucun changement d'adresse IP sur votre réseau.
- Compatibilité avec IPX (réseau Novell), NetBIOS sous Netbeui, Appletalk ou IPv6.
- Pas de translation d'adresses, donc gain de temps au niveau du traitement des paquets par le firewall.

Ce mode est donc préconisé entre la zone externe et la/les DMZ. Il permet de conserver un adressage public sur la zone externe du firewall et les serveurs publics de la DMZ.

Mode hybride

En mode hybride : certaines interfaces possèdent la même adresse IP et d'autres ont une adresse distincte.
Le mode hybride utilise une combinaison des deux modes précédents. Ce mode ne peut être employé que pour les produits NETASQ possédant plus de deux interfaces réseau. Vous pouvez définir plusieurs interfaces en mode transparent.

Exemple

Zone interne et DMZ ou zone externe et DMZ) et certaines interfaces dans un plan d'adressage différent. Ainsi vous avez une plus grande flexibilité dans l'intégration du produit.

Conclusion

Le choix d'un mode se fait uniquement au niveau de la configuration des interfaces réseau. La configuration du firewall est ensuite la même pour tous les modes.
Au niveau sécurité, tous les modes de fonctionnement sont identiques. On filtre les mêmes choses et la détection d'attaques est identique.

Présentation de l'écran de configuration

L'écran de configuration des interfaces se décompose en 3 parties :

- **L'arborescence des interfaces** : les interfaces du boîtier sont présentées de manière triée, c'est-à-dire dans l'ordre suivant : Bridge, Interface, VLAN, Modem en fonction de la vue choisie. Un simple clic sur une interface permet d'afficher sa configuration. Il est possible également d'utiliser le moteur de recherche pour rechercher une interface spécifique. (Exemple : en saisissant « br », tous les bridges sont indiqués).
- **Le panneau de configuration** (panneau central) : en cliquant sur une interface via l'arborescence des interfaces, sa configuration s'affiche dans ce panneau.
- **La barre d'outils** : cette barre permet :
  - d'ajouter ou de supprimer des interfaces (bridge, modem),
  - d'étendre ou de réduire l'arborescence des interfaces,
  - de choisir selon 3 types de vue : « Vue mixte » qui est la vue par défaut et qui correspond à une représentation logique des interfaces (c'est-à-dire les bridges d'abord (qui sont le nœud racine), les interfaces, les vlans (attachés à l'interface ou au bridge) puis les modems), « Grouper par port physique » et « Grouper par plan d'adressage »), de filtrer selon l'interface souhaitée et de vérifier l'utilisation (check).

Arborescence des interfaces

Les interfaces du boîtier sont indiquées dans l'arborescence.

Glisser-déposer

Un drag&drop d'une interface modifie sa configuration (ses relations et son plan d'adressage). Si le drag&drop est autorisé, dans ce cas une coche verte est indiquée. Au contraire, si le déplacement est interdit, une icône d'interdiction est indiquée.
Lorsqu'une interface est détachée d'un bridge, une fenêtre permettant de renseigner le plan d'adressage s'affiche.
Les déplacements possibles sont indiqués dans le tableau suivant :

Bridge/Interface	De	Vers
Interface Ethernet	Bridge	Racine
Interface Ethernet	Bridge	Autre bridge
Interface Ethernet	Racine	Bridge
Vlan	Interface Ethernet	Autre interface Ethernet
Vlan	Interface Ethernet	Bridge
Vlan	Bridge	Autre bridge
Vlan	Bridge	Interface Ethernet
Modem (PPPoE)	Interface	Autre interface

Recherche d'interfaces

Il est possible de retrouver une interface plus facilement grâce au champ de recherche.
La recherche est possible sur les champs de l'interface Nom, Adresse, Type, Commentaire, Hostname (DHCP), Adresse physique MAC, Passerelle (routage par interface).

Exemple : Vous pouvez rechercher une interface en indiquant son nom ou encore l'adresse de sa passerelle.

Pour valider une recherche, il suffit de cliquer sur **Entrée**. Pour supprimer la recherche, il suffit de cliquer sur la croix à droite du champ de recherche.

Identification des interfaces

Chaque interface possède sa propre icône pour une identification visuelle plus immédiate. Cette icône permet également un repérage de l'état de l'interface selon qu'elle est désactivée ou non. Dans le cas d'une désactivation, l'icône et le nom de l'interface sont grisées.
Les interfaces ethernets possèdent un nom propre (ex : "Out") et un nom technique (ex : "0"). Le port physique est affiché entre crochets après le nom des interfaces.

La barre d'outils

Ajouter	Ce bouton vous permet d'ouvrir l'assistant de création d'un bridge, d'un vlan ou encore d'un modem.
Supprimer	Ce bouton vous permet de supprimer une interface préalablement sélectionnée dans l'arborescence des interfaces. Les interfaces Ethernet ne peuvent être supprimées.
Réduire	Ce bouton permet de regrouper l'arborescence des interfaces.
Développer	Ce bouton permet d'étendre l'arborescence des interfaces.

Vue mixte	3 vues sont proposées : **Vue mixte**, **Grouper par port physique** (les interfaces sont regroupées par port. Pour chaque port, les interfaces et les vlan sont indiqués), **Grouper par plan d'adressage** (les interfaces sont séparées selon leur plan d'adressage. Si l'interface contient une adresse + un alias, dans ce cas, elle sera affichée 2 fois dans l'arborescence).
Tout afficher	5 choix sont proposés pour filtrer : **Bridge**, **Interface**, **VLAN**, **Modem (Dialup)**, **Tout afficher**.
Vérifier l'utilisation	Si vous cliquez sur ce bouton après avoir sélectionné une interface, le résultat s'affiche dans l'arborescence des modules. Si vous supprimez une interface, une vérification est faite afin de prévenir l'utilisateur des configurations qui utilisent l'interface qu'il souhaite supprimer. Si l'interface est utilisée, dans ce cas un message s'affiche : *« **Attention**, cette interface/bridge est utilisée par un ou plusieurs modules. La supprimer peut rendre le firewall instable* ». Vous pouvez alors forcer la suppression, vérifier l'utilisation ou annuler. Dans le cas où le résultat de la vérification est négatif, le message : « Voulez-vous réellement supprimer cette interface ? » s'affiche.

A partir de la version 9.0.1, un modem 3G externe peut être connecté au port USB.

Un message d'avertissement s'affichera lorsqu'une interface sera renommée.

 **NOTE**

Le renommage d'une interface ne migre pas les références à celle-ci en particulier dans les éléments de configuration utilisant les objets générés tel que "Network_in" par exemple.

Modifications d'un Bridge

Pour modifier les paramètres d'un bridge, cliquez sur son libellé dans la partie gauche de la fenêtre. Trois onglets permettent la modification des paramètres du bridge.

Onglet « Général »

Nom (obligatoire)	Nom utilisateur de l'interface. Ce nom doit être unique et contenir 16 caractères au maximum. Le nom du bridge ne peut contenir certaines appellations (*Cf. Annexe M* pour connaître les « Noms interdits »).
Commentaire	Permet de donner un commentaire pour l'interface.

Membres du bridge

Ports physiques	Liste des ports Ethernet contenus dans le bridge (Exemple : (Port2)
Interfaces (physiques et logiques)	Liste des interfaces contenues dans le bridge (Exemple : in)

Plan d'adressage

IP dynamique (obtenue par DHCP)	Lorsque votre firewall ne possède pas d'adresse IP statique (son adresse IP est renouvelée régulièrement par votre fournisseur d'accès, DHCP, etc.), il est possible d'associer via un fournisseur de services DNS (**dyndns.org** par exemple) l'adresse IP allouée et un nom de domaine (qui lui est fixe) afin de pouvoir contacter ce firewall sans pour autant connaître son adresse IP. Cette option vous permet d'activer cette fonctionnalité en sélectionnant un compte DNS dynamique que vous avez préalablement configuré. *Pour plus d'informations concernant le client DNS dynamique, veuillez-vous référer au module DNS Dynamique.* Ce champ permet de spécifier au firewall que la configuration du bridge (adresse IP et masque) est définie par DHCP. Dans ce cas, la zone « DHCP » de l'onglet `Configuration avancée` est active.
IP fixe (statique)	Votre firewall possède ici une adresse IP statique (fixe).

Liste d'adresses IP du bridge

Ce tableau s'affiche si l'option **IP fixe (statique**) a été cochée.

Adresse IP	Adresse IP affectée au bridge. (Toutes les interfaces contenues dans le bridge possèdent la même adresse IP).
Masque réseau	Masque de réseau du sous-réseau auquel appartient le bridge. Les différentes interfaces faisant partie du bridge ont la même adresse IP donc tous les réseaux connectés au firewall font partie du même plan d'adressage. Le masque de réseau donne au firewall les informations sur le réseau dont il fait partie.
Commentaire	Permet de spécifier un commentaire pour l'adressage du bridge.

Ici, plusieurs adresses IP et masques associés peuvent être définis pour le même bridge (besoin de création d'alias par exemple). Ces alias peuvent vous permettre d'utiliser ce firewall NETASQ comme un point de routage central. De ce fait, un bridge peut être connecté à différents sous-réseaux ayant un adressage différent. Pour les ajouter ou les retirer, il suffit d'utiliser les boutons d'action **Ajouter** et **Supprimer** situés au-dessus des champs du tableau.

Onglet « Configuration avancée »

MTU	Longueur maximale (en octets) des trames émises sur le support physique (Ethernet) afin que celles-ci soient transmises en une seule fois (donc sans fragmentation).
Adresse physique (MAC)	**AVERTISSEMENT** Cette option n'est pas accessible pour les firewalls en Haute Disponibilité. Cette option vous permet de spécifier une adresse MAC pour une interface plutôt que d'utiliser l'adresse allouée par le firewall. Cela vous permet de faciliter d'autant plus l'intégration en mode transparent de votre firewall NETASQ dans votre réseau (en spécifiant l'adresse MAC de votre routeur plutôt que d'avoir à reconfigurer tous les postes utilisant cette adresse MAC).Lorsque l'adresse MAC est affectée au bridge, toutes les interfaces contenues dans ce bridge possèdent alors la même adresse MAC. Cette adresse se compose de 6 octets en hexadécimal séparés par des :

DHCP



NOTE

Indication « désactivé » si l'option IP dynamique (obtenue par DHCP) n'est pas cochée dans l'onglet `Général` et les options sont grisées.

Nom DNS (facultatif)	Nom du serveur DNS (FQDN) pour la connexion. Ce champ facultatif, n'identifie pas le serveur DHCP mais le firewall. Si le champ est rempli et que le serveur DHCP externe possède l'option de mise à jour automatique du serveur DNS, alors le serveur DHCP met à jour automatiquement le serveur DNS avec le nom fourni par le firewall et l'adresse IP qui lui a été fournie. Ce nom se compose de 6 octets en hexadécimal séparés par des :
Durée de bail demandée (secondes)	Période de conservation de l'adresse IP avant renégociation.
Demander les serveurs DNS au serveur DHCP et créer les objets machines	Lorsque cette option est cochée, le firewall récupère les serveurs DNS auprès du serveur DHCP (fournisseur d'accès par exemple) qu'il contacte pour obtenir son adresse IP. Dès que cette option est cochée deux objets sont dynamiquement créés dans la base d'objets : Firewall_<nom de l'interface>_dns1 et Firewall_<nom de l'interface_dns2. Ils peuvent ainsi être utilisés dans la configuration du service DHCP. Ainsi si le firewall offre un service DHCP aux utilisateurs de son réseau, les utilisateurs seront crédités des serveurs DNS fournis par le fournisseur d'accès.

Onglet « Membres du Bridge »

Une autre manière d'inclure des interfaces dans un bridge, hormis le drag'n drop consiste à utiliser le panneau de cet onglet (membre du bridge).
Pour déplacer une interface disponible dans le bridge, réalisez un drag'n drop ou utilisez la flèche rouge au centre des 2 tableaux ou encore double-cliquez sur l'interface à déplacer.
Pour retirer une interface du bridge, faites la même manipulation dans le sens inverse.

Création d'un bridge

La création d'un Bridge est réalisée au moyen d'un assistant vous permettant de créer de manière simple l'interface.

Cliquez sur le bouton **Ajouter** de la barre d'outils puis sélectionnez « Ajouter un Bridge ». L'écran de création d'un nouveau bridge s'affiche.



NOTE

Le nombre de bridges à créer varie selon votre modèle de firewall.

Identification du bridge

Nom	Nom utilisateur de l'interface. Ce nom doit être unique et contenir 16 caractères au maximum. Le nom du bridge ne peut contenir certaines appellations.
Commentaire	Permet de donner un commentaire pour l'interface.

Plan d'adressage

IP fixe (statique)	En cochant cette option, le bridge a un adressage statique. Il faut dans ce cas indiquer son adresse IP et le masque de réseau du sous-réseau auquel appartient le bridge.
IP dynamique (obtenue par DHCP)	En cochant cette option, l'interface est définie par DHCP. Il faut dans ce cas indiquer un nom d'hôte DHCP qui est un nom de serveur (FQDN) pour la connexion. Ce champ facultatif, n'identifie pas le serveur DHCP mais le firewall. Si le champ est rempli et que le serveur DHCP externe possède l'option de mise à jour automatique du serveur DNS, alors le serveur DHCP met à jour automatiquement le serveur DNS avec le nom fourni par le firewall et l'adresse IP qui lui a été fournie. et le temps alloué (obligatoire). Ce nom se compose de 6 octets en hexadécimal séparés par des : Il faut également indiquer une période de conservation de l'adresse IP avant renégociation.

Cliquez sur **Suivant** au bas de l'écran. L'écran de création du bridge (étape 2) s'affiche.
Sélectionnez les interfaces pour lesquelles vous souhaitez réaliser un bridge. La liste "Interfaces disponibles" recense les Ethernets et les vlan déjà présents dans la configuration. Il faut sélectionner au moins deux interfaces qui composeront le bridge, soit par l'intermédiaire des flèches, soit en effectuant un drag'n drop entre les deux listes ou encore en double-cliquant sur l'interface. Cliquez sur **Terminer** pour valider la création.

Suppression d'un bridge

Pour supprimer un bridge, sélectionnez-le dans l'arborescence des interfaces, puis cliquez sur le bouton **Supprimer** de la barre d'outils. Le message « *Voulez-vous réellement supprimer cette interface ?* » s'affiche.
Confirmez ou non votre suppression.
Si vous confirmez la suppression, une vérification est faite (check) pour voir si l'interface est utilisée.

 **NOTE**
La suppression d'un bridge désactive les interfaces qu'il contenait ainsi que le passage de celles-ci vers une configuration en DHCP.

Modification d'une interface Ethernet (en mode Bridge)

Une interface appartenant à un bridge est représentée sous forme de nœud fils par rapport au bridge. Un bridge peut donc contenir plusieurs nœuds fils.
Vous pouvez modifier les paramètres de chaque interface appartenant ou non au bridge. Pour cela, sélectionnez une interface située sous un bridge en en dehors du bridge dans la partie gauche de la fenêtre. Deux onglets s'affichent :

 **NOTE**
Il n'est pas possible d'ajouter ou de supprimer des interfaces Ethernet.

Onglet « Configuration de l'interface »

Nom (obligatoire)	Nom associé à l'interface du bridge. Ce nom doit être unique et contenir 16 caractères au maximum. Le nom de l'interface du bridge ne peut contenir certaines appellations.
Commentaire	Permet de donner un commentaire pour l'interface.
Port physique	Nom du port physique (exemple : in (port 2)).
VLAN(s) attaché(s) à l'interface	Liste des VLANs attachés à l'interface sélectionnée. ***A partir de la version 9.0.1,*** il ne vous est plus systématiquement demandé de redémarrer le boîtier lors de la suppression d'un VLAN.
Couleur	Couleur attribuée à l'interface.
Cette interface est	Si vous sélectionnez « interne (protégée) », vous indiquez le caractère privé de l'interface. Les adresses des interfaces **internes** ne sont pas utilisables en tant que destination pour les paquets en provenance des interfaces non protégées, hormis si ceux-ci viennent d'être translatés. **NOTE** On notera que « interne (protégée) » implique forcément d'être sur une interface protégée. Les options « interne (protégée) **»** et « externe (publique) » sont donc incompatibles. Si vous sélectionnez l'option « externe (publique) », vous indiquez que cette partie du réseau est reliée à Internet. Dans la majorité des cas, l'interface externe, reliée à Internet, doit être en mode externe. Le caractère protégé de l'interface matérialisé par un bouclier ( ), disparaît lorsque cette option est cochée.

Plan d'adressage

Aucun (interface désactivée)	En cochant/décochant cette option on active/désactive l'interface. En désactivant une interface, on la rend inutilisable. En terme d'utilisation cela peut correspondre à une interface que l'on a prévu de déployer dans un futur proche ou éloigné mais qui n'est pas en activité. Une interface désactivée car non utilisée est une mesure de sécurité supplémentaire contre les intrusions.
IP dynamique (obtenue par DHCP)	Lorsque votre firewall ne possède pas d'adresse IP statique (son adresse IP est renouvelée régulièrement par votre fournisseur d'accès, DHCP, etc.), il est possible d'associer via un fournisseur de services DNS (**dyndns.org** par exemple) l'adresse IP allouée et un nom de domaine (qui lui est fixe) afin de pouvoir contacter ce firewall sans pour autant connaître son adresse IP. Cette option vous permet d'activer cette fonctionnalité en sélectionnant un compte DNS dynamique que vous avez préalablement configuré. *Pour plus d'informations au sujet du client DNS dynamique, veuillez-vous référer au module DNS dynamique.* Ce champ permet donc de spécifier au firewall que la configuration du bridge (adresse IP et masque) est définie par DHCP. Dans ce cas, la zone « DHCP » de l'onglet `Configuration avancée` est active.
Plan d'adressage hérité du Bridge	Si l'interface fait partie d'un bridge, dans ce cas, il est possible de récupérer le plan d'adressage du bridge.
IP fixe (statique)	En cochant cette option, l'interface a un adressage statique. Il faut dans ce cas indiquer son adresse IP et le masque de réseau du sous-réseau auquel appartient l'interface.

Onglet « Configuration avancée »

MTU	Longueur maximale (en octets) des paquets émis sur le support physique (Ethernet) afin que ceux-ci soient transmis en une seule fois (donc sans fragmentation). Ce choix n'est pas disponible pour une interface contenue dans un bridge.
Adresse physique (MAC)	**AVERTISSEMENT** Cette option n'est pas accessible pour les firewalls en Haute Disponibilité. Cette option vous permet de spécifier une adresse MAC pour une interface plutôt que d'utiliser l'adresse allouée par le firewall. Cela vous permet de faciliter d'autant plus l'intégration en mode transparent de votre firewall NETASQ dans votre réseau (en spécifiant l'adresse MAC de votre routeur plutôt que d'avoir à reconfigurer tous les postes utilisant cette adresse MAC). Si l'interface est contenue dans un bridge, dans ce cas, elle possède la même adresse MAC que lui.  **NOTE** Ce champ est grisé lorsque l'interface appartient à un bridge. Il n'est ni modifiable, ni supprimable.

DHCP

 **NOTE**

Indication « désactivé » si l'option **IP dynamique (obtenue par DHCP)** n'est pas cochée dans l'onglet **`Configuration de l'interface`** et les options sont grisées.

Nom DNS (facultatif)	Nom du serveur DNS (FQDN) pour la connexion. Ce champ facultatif, n'identifie pas le serveur DHCP mais le firewall. Si le champ est rempli et que le serveur DHCP externe possède l'option de mise à jour automatique du serveur DNS, alors le serveur DHCP met à jour automatiquement le serveur DNS avec le nom fourni par le firewall et l'adresse IP qui lui a été fournie. Ce nom se compose de 6 octets en hexadécimal séparés par des :
Durée de bail demandée	Période de conservation de l'adresse IP avant renégociation.
Demander les serveurs DNS au serveur DHCP et créer les objets machine associés	Lorsque cette option est cochée, le firewall récupère les serveurs DNS auprès du serveur DHCP (fournisseur d'accès par exemple) qu'il contacte pour obtenir son adresse IP. Dès que cette option est cochée deux objets sont dynamiquement créés dans la base d'objets : Firewall_<nom de l'interface>_dns1 et Firewall_<nom de l'interface_dns2. Ils peuvent ainsi être utilisés dans la configuration du service DHCP. Ainsi si le firewall offre un service DHCP aux utilisateurs de son réseau, les utilisateurs seront crédités des serveurs DNS fournis par le fournisseur d'accès.  **NOTE** Cette option est désactivée si l'option **IP dynamique (obtenue par DHCP)** n'est pas activée dans l'onglet `Configuration de l'interface`.

Bridge – Routage sans analyse

 **NOTE**

Indication « désactivé » si l'option **Plan d'adressage hérité du bridge** n'est pas cochée dans l'onglet **`Configuration de l'interface`** et les options sont grisées.

Autoriser sans analyser	Permet de laisser passer les paquets IPX (réseau Novell), NetBIOS (sur NETBEUI), paquets AppleTalk (pour les machines Macintosh), PPPoe ou IPv6 entre les interfaces du pont. Aucune analyse ou aucun filtrage de niveau supérieur n'est réalisé sur ces protocoles (le firewall bloque ou laisse passer).

Bridge – Routage par interface

 **NOTE**

Indication « désactivé » si l'option **Plan d'adressage hérité du bridge** n'est pas cochée dans l'onglet **`Configuration de l'interface`** et les options sont grisées.

Préserver le routage initial	Comme son nom l'indique, cette option permet de préserver le routage initial des machines connectées sur cette interface. Ainsi vous pouvez spécifier une passerelle par défaut pour certaines machines tout en spécifiant sur le firewall une passerelle pour celles qui n'en ont pas. Cette option facilite l'intégration du firewall dans une architecture composée de nombreuses passerelles différentes.
Préserver les identifiants de Vlan	Cette option permet la transmission des trames taguées sans que le firewall soit une terminaison du VLAN. Le tag VLAN de ces trames est conservé ainsi le firewall peut être placé sur le chemin d'un VLAN sans pour autant que ce VLAN soit coupé par le firewall. Le firewall agit de manière complètement transparente pour ce VLAN.
Adresse de la passerelle	Ce champ sert au routage par interface. Tous les paquets arrivant sur cette interface seront routés via une passerelle.

Média

Média	Vitesse de liaison du réseau. Par défaut le firewall détecte le média automatiquement mais vous pouvez forcer l'utilisation d'un mode particulier. Les vitesses proposées sont : "Détection automatique", "10 Mb Half duplex", "10 Mb Full duplex", "100 Mb Half duplex", "100 Mb Full duplex", "1 Gbps Full duplex".  **AVERTISSEMENT** Si le firewall est directement connecté à un modem ADSL, NETASQ vous recommande de forcer le média que vous voulez utiliser sur l'interface en question.

Bande passante de l'interface (informatif)

Bande passante	Définit le débit sur une interface. Il s'agit d'une entrée automatique, non obligatoire : sert au monitoring pour le calcul de la bande passante).

Modification d'une interface Ethernet (en mode avancé)

Pour configurer une interface dans un réseau ne faisant pas partie d'un bridge, il suffit de la sortir de l'arborescence du bridge avec la souris. Vous pouvez ensuite configurer les paramètres de l'interface. Lors du détachement, l'écran de plan d'adressage s'affiche.

IP fixe (statique)	En cochant cette option, l'interface a un adressage statique. Il faut dans ce cas indiquer son adresse IP et le masque réseau.
IP dynamique (obtenue par DHCP)	En cochant cette option, l'interface est définie par DHCP. Il faut dans ce cas indiquer un nom d'hôte DHCP et une durée de bail.

Modification d'un Vlan

Onglet « Configuration de l'interface »

Nom (obligatoire)	Nom associé au Vlan. Ce nom doit être unique et contenir 16 caractères au maximum. Le nom du Vlan ne peut contenir certaines appellations.
Commentaire	Permet de donner un commentaire pour le Vlan.
Interface parente	Nom physique de l'interface à laquelle est attaché le Vlan.
Couleur	Couleur attribuée au Vlan.
Identifiant de VLAN	Identifiant du Vlan qui peut être compris entre 1 et 4094 et doit être unique (sauf s'il s'agit d'un Vlan associé à un autre bridge dans un vlan traversant).
Cette interface est	Si vous sélectionnez « interne (protégée) », vous indiquez le caractère privé de l'interface. Les adresses des interfaces **internes** ne sont pas utilisables en tant que destination pour les paquets en provenance des interfaces non protégées, hormis si ceux-ci viennent d'être translatés. **NOTE** On notera que « interne (protégée) » implique forcément d'être sur une interface protégée. Les options « interne (protégée) **»** et « externe (publique) » sont donc incompatibles. Si vous sélectionnez l'option « externe (publique) », vous indiquez que cette partie du réseau est reliée à Internet. Dans la majorité des cas, l'interface externe, reliée à Internet, doit être en mode externe. Le caractère protégé de l'interface matérialisé par un bouclier ( ) disparaît lorsque cette option est cochée.

Plan d'adressage

Aucun (interface désactivée)	En cochant/décochant cette option on active/désactive l'interface. En désactivant une interface, on la rend inutilisable. En terme d'utilisation cela peut correspondre à une interface que l'on a prévu de déployer dans un futur proche ou éloigné mais qui n'est pas en activité. Une interface désactivée car non utilisée est une mesure de sécurité supplémentaire contre les intrusions.
IP dynamique (obtenue par DHCP)	Lorsque votre firewall ne possède pas d'adresse IP statique (son adresse IP est renouvelée régulièrement par votre fournisseur d'accès, DHCP, etc.), il est possible d'associer via un fournisseur de services DNS (**dyndns.org** par exemple) l'adresse IP allouée et un nom de domaine (qui lui est fixe) afin de pouvoir contacter ce firewall sans pour autant connaître son adresse IP. Cette option vous permet d'activer cette fonctionnalité en sélectionnant un compte DNS dynamique que vous avez préalablement configuré. *Pour plus d'informations au sujet du client DNS dynamique, veuillez-vous référer au module DNS dynamique.* Ce champ permet donc de spécifier au firewall que la configuration du bridge (adresse IP et masque) est définie par DHCP. Dans ce cas, la zone « DHCP » de l'onglet `Configuration avancée` est active.
Plan d'adressage hérité du Bridge	Si l'interface fait partie d'un bridge, dans ce cas, il est possible de récupérer le plan d'adressage du bridge. La zone est grisée si l'interface n'appartient pas à un bridge.
IP fixe (statique)	En cochant cette option, l'interface a un adressage statique. Il faut dans ce cas indiquer son adresse IP et le masque de réseau du sous-réseau auquel appartient l'interface.

Onglet « Configuration avancée »

MTU	Longueur maximale (en octets) des paquets émis sur le support physique (Ethernet) afin que ceux-ci soient transmis en une seule fois (donc sans fragmentation). Ce choix n'est pas disponible pour une interface contenue dans un bridge.
Adresse physique (MAC)	 **AVERTISSEMENT** Cette option n'est pas accessible pour les firewalls en Haute Disponibilité. Cette option vous permet de spécifier une adresse MAC pour une interface plutôt que d'utiliser l'adresse allouée par le firewall. Cela vous permet de faciliter d'autant plus l'intégration en mode transparent de votre firewall NETASQ dans votre réseau (en spécifiant l'adresse MAC de votre routeur plutôt que d'avoir à reconfigurer tous les postes utilisant cette adresse MAC). Si l'interface est contenue dans un bridge, dans ce cas, elle possède la même adresse MAC que lui.  **NOTE** Ce champ est grisé lorsque l'interface appartient à un bridge.

DHCP

 **NOTE**

Indication « désactivé » si l'option **IP dynamique (obtenue par DHCP)** n'est pas cochée dans l'onglet **`Configuration de l'interface`** et les options sont grisées.

Nom DNS (facultatif)	Nom du serveur DNS (FQDN) pour la connexion. Ce champ facultatif, n'identifie pas le serveur DHCP mais le firewall. Si le champ est rempli et que le serveur DHCP externe possède l'option de mise à jour automatique du serveur DNS, alors le serveur DHCP met à jour automatiquement le serveur DNS avec le nom fourni par le firewall et l'adresse IP qui lui a été fournie. Ce nom se compose de 6 octets en hexadécimal séparés par des :
Durée de bail demandée	Période de conservation de l'adresse IP avant renégociation.
Demander les serveurs DNS au serveur DHCP et créer les objets machine associés	Lorsque cette option est cochée, le firewall récupère les serveurs DNS auprès du serveur DHCP (fournisseur d'accès par exemple) qu'il contacte pour obtenir son adresse IP. Dès que cette option est cochée deux objets sont dynamiquement créés dans la base d'objets : Firewall_<nom de l'interface>_dns1 et Firewall_<nom de l'interface_dns2. Ils peuvent ainsi être utilisés dans la configuration du service DHCP. Ainsi si le firewall offre un service DHCP aux utilisateurs de son réseau, les utilisateurs seront crédités des serveurs DNS fournis par le fournisseur d'accès.  **NOTE** Cette option est désactivée si l'option **IP dynamique (obtenue par DHCP)** n'est pas activée dans l'onglet `Configuration de l'interface`.

Bridge – Routage sans analyse

 **NOTE**

Indication « désactivé » si l'option **Plan d'adressage hérité du bridge** n'est pas cochée dans l'onglet **`Configuration de l'interface`** et les options sont grisées.

Autoriser sans analyser	Permet de laisser passer les paquets IPX (réseau Novell), NetBIOS (sur NETBEUI), paquets AppleTalk (pour les machines Macintosh), PPPoe ou IPv6 entre les interfaces du pont. Aucune analyse ou aucun filtrage de niveau supérieur n'est réalisé sur ces protocoles (le firewall bloque ou laisse passer).

Bridge – Routage par interface

 **NOTE**

Indication « désactivé » si l'option **Plan d'adressage hérité du bridge** n'est pas cochée dans l'onglet **`Configuration de l'interface`** et les options sont grisées.

Préserver le routage initial	Comme son nom l'indique, cette option permet de préserver le routage initial des machines connectées sur cette interface. Ainsi vous pouvez spécifier une passerelle par défaut pour certaines machines tout en spécifiant sur le firewall une passerelle pour celles qui n'en ont pas. Cette option facilite l'intégration du firewall dans une architecture composée de nombreuses passerelles différentes.
Adresse de la passerelle	Ce champ sert au routage par interface. Tous les paquets arrivant sur cette interface seront routés via une passerelle.

Bande passante de l'interface (informatif)

Bande passante	Définit le débit sur une interface. Il s'agit d'une entrée automatique, non obligatoire : sert au monitoring pour le calcul de la bande passante).

Création d'un Vlan

La configuration d'un VLAN est réalisée au moyen d'un assistant vous permettant de créer de manière simple l'interface.

Sélectionnez l'interface ou le bridge auquel vous désirez associer un VLAN. Puis cliquez sur le bouton **Ajouter** puis **Ajouter un VLAN**.

Choisissez ensuite le type de VLAN que vous souhaitez créer :

VLAN attaché à une seule interface (extrémité de VLAN)	Les firewalls multifonctions NETASQ peuvent se placer en terminaison de VLAN pour ajouter ou retirer un tag VLAN. Le firewall assure le filtrage entre VLAN et assure les communications entre les VLAN et les réseaux connectés aux autres interfaces du firewall. Les VLAN sont perçus par le firewall comme appartenant à des interfaces virtuelles, ce qui permet leur totale intégration au sein du système de sécurité de l'entreprise. Si vous sélectionnez cette option, en cliquant sur **Suivant**, l'écran d'étape 2 s'affiche. La création se passe en deux étapes.
VLAN attaché à 2	Cette option permet de créer un vlan traversant, c'est-à-dire un bridge

interfaces (VLAN traversant)	contenant 2 Vlan ayant un identifiant identique. Si vous sélectionnez cette option, en cliquant sur le bouton **Suivant**, l'écran d'étape 3 s'affiche.

VLAN attaché à une seule interface (extrémité de VLAN)

Identification du VLAN

Interface parente	Sélectionnez l'interface sur laquelle sera attaché le VLAN.
Nom	Saisissez un nom unique pour votre VLAN *(Cf. Annexe M : Noms interdits*).
Commentaire	Vous pouvez également donner une description.
Couleur	Couleur attribuée au VLAN.
Identifiant de VLAN	Ce champ permet de spécifier quelle sera la valeur associée au VLAN dans les paquets transitant sur le réseau. Ce tag identifie le VLAN et est utilisé au niveau Ethernet. Il doit être unique et compris entre 1 et 4094.
Ce VLAN est	Déterminez si vous souhaitez une interface externe ou interne.

Plan d'adressage

IP dynamique (obtenue par DHCP)	Cochez cette option pour donner une adresse dynamique au VLAN.
IP fixe (statique)	En cochant cette option, l'interface a un adressage statique. Il faut dans ce cas indiquer son adresse IP et le masque réseau.

Cliquez sur **Terminer.**

VLAN attaché à 2 interfaces (VLAN traversant)

Dans la configuration des VLAN pour les bridges, il est possible d'utiliser le même tag pour deux interfaces VLAN. Ainsi le firewall apparaît de manière transparente sur le réseau. Cette méthode nécessite l'utilisation d'une interface VLAN par interface physique concernée.
Contrairement à l'option **Préserver les identifiants de VLAN** (*cf. dans la configuration avancée d'une interface Ethernet*) qui rend le firewall complètement transparent par rapport au VLAN et qui empêche donc l'utilisation de fonctionnalités qui consisterait à couper le flux VLAN, par exemple les proxies, cette méthode de préservation du tag VLAN entre plusieurs interfaces d'un même bridge permet l'utilisation complète des fonctionnalités du firewall.

Identification du VLAN

Nom	Saisissez un nom unique pour votre VLAN.
Identifiant de VLAN	Ce champ permet de spécifier quelle sera la valeur associée au VLAN dans les paquets transitant sur le réseau. Ce tag identifie le VLAN et est utilisé au niveau Ethernet.
Couleur	Couleur attribuée au VLAN.

Plan d'adressage du VLAN

Utiliser un bridge existant	En cochant cette option, vous sélectionnez dans la liste déroulante le bridge auquel seront attachés les Vlan.
Créer un nouveau bridge	En cochant cette option, un wizard permettra de créer un nouveau bridge qui contiendra donc les deux interfaces.
IP dynamique (obtenue par DHCP)	Lorsque votre firewall ne possède pas d'adresse IP statique (son adresse IP est renouvelée régulièrement par votre fournisseur d'accès, DHCP, etc.), il est possible d'associer via un fournisseur de services DNS (**dyndns.org** par exemple) l'adresse IP allouée et un nom de domaine (qui lui est fixe) afin de pouvoir contacter ce firewall sans pour autant connaître son adresse IP. Cette option vous permet d'activer cette fonctionnalité en sélectionnant un compte DNS dynamique que vous avez préalablement configuré. Veuillez-vous référer au module DNS dynamique pour plus d'informations sur la configuration du client DNS dynamique. Ce champ permet donc de spécifier au firewall que la configuration du bridge (adresse IP et masque) est définie par DHCP. Dans ce cas, la zone « DHCP » de l'onglet `Configuration avancée` est active.
IP fixe (statique)	En cochant cette option, l'interface a un adressage statique. Il faut dans ce cas indiquer son adresse IP et le masque de réseau du sous-réseau auquel appartient l'interface.

Cliquez sur **Suivant**.

Identification du VLAN entrant

Nom (obligatoire)	Nom unique pour votre VLAN. Ce champ est pré-rempli en fonction du nom indiqué dans le champ Nom de l'étape 3 suffixé par « 1 ».
Interface (obligatoire)	Sélectionnez l'interface sur laquelle sera attaché le VLAN.
Ce VLAN est	Si vous sélectionnez « interne (protégée) », vous indiquez le caractère privé de l'interface. Les adresses des interfaces **internes** ne sont pas utilisables en tant que destination pour les paquets en provenance des interfaces non protégées, hormis si ceux-ci viennent d'être translatés. **NOTE** On notera que « interne (protégée) » implique forcément d'être sur une interface protégée. Les options « interne (protégée) **»** et « externe (publique) » sont donc incompatibles. **Si vous sélectionnez l'option « externe (publique) »,** vous indiquez que cette partie du réseau est reliée à Internet. Dans la majorité des cas, l'interface externe, reliée à Internet, doit être en mode externe. Le caractère protégé de l'interface, matérialisé par un bouclier ( ), disparaît lorsque cette option est cochée.

*Cliquez de nouveau sur **Suivant.***

Identification du VLAN sortant

Nom (obligatoire)	Nom unique pour votre VLAN. Ce champ est pré-rempli en fonction du nom indiqué dans le champ Nom de l'étape 3 suffixé par « _2 ».
Interface	Saisissez un nom unique pour votre VLAN.
Ce VLAN est	Si vous sélectionnez « interne (protégée) », vous indiquez le caractère privé de l'interface. Les adresses des interfaces **internes** ne sont pas utilisables en tant que destination pour les paquets en provenance des interfaces non protégées, hormis si ceux-ci viennent d'être translatés. **NOTE** On notera que « interne (protégée) » implique forcément d'être sur une interface protégée. Les options « interne (protégée) **»** et « externe (publique) » sont donc incompatibles. **Si vous sélectionnez l'option « externe (publique) »,** vous indiquez que cette partie du réseau est reliée à Internet. Dans la majorité des cas, l'interface externe, reliée à Internet, doit être en mode externe. Le caractère protégé de l'interface matérialisé par un bouclier ( ) disparaît lorsque cette option est cochée.

L'écran suivant résume la configuration que vous venez de réaliser.

Ajout de VLAN

Si vous souhaitez créer un nouveau VLAN et que vous êtes arrivé au maximum du nombre dynamique de VLANs possible, une fenêtre pop-up s'affiche pour en ajouter d'autres. Il est possible également de modifier manuellement ce nombre en allant dans `Système\Configuration\Réseau\VLAN disponibles (max 128)\`.

Suppression d'un Vlan

Pour supprimer un vlan, sélectionnez-le dans l'arborescence des interfaces, puis cliquez sur le bouton **Supprimer** de la barre d'outils. Le message « Voulez-vous réellement supprimer cette interface ? » s'affiche.
Confirmez ou non votre suppression.
En confirmant la suppression, une vérification de l'utilisation de l'interface (check) est faite.

Modification d'un modem

Modem PPPoE

Utiliser ce modem	En cochant cette option, vous activez le modem.
Nom (obligatoire)	Nom associé au modem. Ce nom doit être unique et contenir 16 caractères au maximum. Le nom du modem ne peut contenir certaines appellations.
Commentaire	Permet de donner un commentaire pour le modem.
Type de modem	Indication du type de modem choisi lors de la création.
Couleur	Couleur attribuée au modem.

Authentification

Identifiant	Nom utilisé pour l'authentification
Mot de passe	Mot de passe utilisé pour l'authentification. Si vous cliquez sur l'icône « clé » à droite de ce champ, le mot de passe s'affiche en clair pour une durée de 5 secondes.

Connectivité

Le modem est connecté à l'interface	Indication de l'interface de connexion du modem.
Demander les serveurs DNS et créer les objets machines associés	Lorsque cette option est cochée, le firewall récupère les serveurs DNS auprès du serveur DHCP (fournisseur d'accès par exemple) qu'il contacte pour obtenir son adresse IP. Dès que cette option est cochée deux objets sont dynamiquement créés dans la base d'objets : Firewall_<nom de l'interface>_dns1 et Firewall_<nom de l'interface_dns2. Ils peuvent ainsi être utilisés dans la configuration du service DHCP. Ainsi si le firewall offre un service DHCP aux utilisateurs de son réseau, les utilisateurs seront crédités des serveurs DNS fournis par le fournisseur d'accès.

Configuration avancée

Service	Type de service PPPoe utilisé. Cette option permet de différencier plusieurs modems ADSL. Par défaut, laissez ce champ vide.
Connexion	La connexion en cas de trafic (à la demande) n’établit la connexion avec Internet que lorsqu’une demande de connexion émane du réseau interne (ce mode est plus économique dans le cas d’une liaison payante à la durée). La connexion Permanente conserve la connexion vers l’Internet active en permanence.

Modem PPTP

Utiliser ce modem	En cochant cette option, vous activez le modem.
Nom (obligatoire)	Nom associé au modem. Ce nom doit être unique et contenir 16 caractères au maximum. Le nom du modem ne peut contenir certaines appellations.
Commentaire	Permet de donner un commentaire pour le modem.
Type de modem	Indication du type de modem choisi lors de la création.
Couleur	Couleur attribuée au modem.

Authentification

Identifiant	Nom utilisé pour l’authentification.
Mot de passe	Mot de passe utilisé pour l’authentification. Si vous cliquez sur l’icône « clé » à droite de ce champ, le mot de passe s’affiche en clair pour une durée de 5 secondes.

Connectivité

Adresse PPTP	Adresse IP interne du modem ADSL.
Demander les serveurs DNS et créer les objets machines associés	Lorsque cette option est cochée, le firewall récupère les serveurs DNS auprès du serveur DHCP (fournisseur d’accès par exemple) qu’il contacte pour obtenir son adresse IP. Dès que cette option est cochée deux objets sont dynamiquement créés dans la base d’objets : Firewall_<nom de l’interface>_dns1 et Firewall_<nom de l’interface_dns2. Ils peuvent ainsi être utilisés dans la configuration du service DHCP. Ainsi si le firewall offre un service DHCP aux utilisateurs de son réseau, les utilisateurs seront crédités des serveurs DNS fournis par le fournisseur d’accès.

Configuration avancée

Connexion	La connexion en cas de trafic (à la demande) n’établit la connexion avec Internet que lorsqu’une demande de connexion émane du réseau interne (ce mode est plus économique dans le cas d’une liaison payante à la durée). La connexion Permanente conserve la connexion vers l’Internet active en permanence.

Modem PPP

Utiliser ce modem	En cochant cette option, vous activez le modem.
Nom (obligatoire)	Nom associé au modem. Ce nom doit être unique et contenir 16 caractères au maximum. Le nom du modem ne peut contenir certaines appellations.
Commentaire	Permet de donner un commentaire pour le modem.
Type de modem	Indication du type de modem choisi lors de la création.
Couleur	Couleur attribuée au modem.

Authentification

Identifiant	Nom utilisé pour l'authentification
Mot de passe	Mot de passe utilisé pour l'authentification. Si vous cliquez sur l'icône « clé » à droite de ce champ, le mot de passe s'affiche en clair pour une durée de 5 secondes.

Connectivité

Numéro à composer	Numéro d'appel chez le fournisseur d'accès.
Demander les serveurs DNS et créer les objets machines associés	Lorsque cette option est cochée, le firewall récupère les serveurs DNS auprès du serveur DHCP (fournisseur d'accès par exemple) qu'il contacte pour obtenir son adresse IP. Dès que cette option est cochée deux objets sont dynamiquement créés dans la base d'objets : Firewall_<nom de l'interface>_dns1 et Firewall_<nom de l'interface_dns2. Ils peuvent ainsi être utilisés dans la configuration du service DHCP. Ainsi si le firewall offre un service DHCP aux utilisateurs de son réseau, les utilisateurs seront crédités des serveurs DNS fournis par le fournisseur d'accès.

Configuration avancée

Chaîne d'initialisation	Chaîne de caractères servant optionnellement à initialiser la connexion.
Connexion	La connexion **en cas de trafic (à la demande)** n'établit la connexion avec Internet que lorsqu'une demande de connexion émane du réseau interne (ce mode est plus économique dans le cas d'une liaison payante à la durée). La connexion **Permanente** conserve la connexion vers l'Internet active en permanence.

Création d'un modem

Les interfaces modem sont utilisées dans le cas de connexions distantes lorsque votre modem est branché directement sur le firewall (port série ou Ethernet). Le firewall accepte tout type de modem (ADSL, RNIS, RTC, ...).
La création de nouvelles interfaces modem se fait grâce à un assistant. Le nombre maximal de modems disponibles sur votre firewall dépend du modèle.

Dans le menu **`Réseau\Interfaces`** cliquez sur le bouton **Ajouter** et sélectionnez « Ajouter un modem »

Etape 1

Identification du modem

Nom	Indiquez un nom (obligatoire).
Commentaire	Description pour identifier la connexion Dialup.
Couleur	Couleur attribuée à la connexion distante.
Demander les serveurs DNS et créer les objets machines associés	Lorsque cette option est cochée, le firewall récupère les serveurs DNS auprès du serveur DHCP (fournisseur d'accès par exemple) qu'il contacte pour obtenir son adresse IP. Dès que cette option est cochée deux objets sont dynamiquement créés dans la base d'objets : Firewall_<nom de l'interface>_dns1 et Firewall_<nom de l'interface_dns2. Ils peuvent ainsi être utilisés dans la configuration du service DHCP. Ainsi si le firewall offre un service DHCP aux utilisateurs de son réseau, les utilisateurs seront crédités des serveurs DNS fournis par le fournisseur d'accès.

Configuration du modem

Choisissez le type de dialup entre PPPoe, PPTP, PPP ou L2TP. L'écran de configuration varie selon le type de dialup.

PPPoE	Sélectionnez l'interface réseau utilisée pour le modem
PPTP	Saisissez l'adresse IP du modem.
PPP	Indiquez le n° de téléphone utilisé pour le dialing.

Authentification

Identifiant	Indication de l'identifiant (obligatoire).
Mot de passe	Indication du mot de passe (obligatoire).
Confirmation du mot de passe	Confirmation du mot de passe.

Une fois l'étape 1 configurée, cliquez sur le bouton **Suivant**.

Etape 2

Routage : utilisation de la passerelle obtenue par le modem

Choisissez si vous souhaitez définir le modem en tant que passerelle.

A la liste des	La machine Firewall_ <nom du modem>_peer est ajoutée parmi les

passerelles principales	passerelles principales. S'il n'y a pas de passerelle principale, un écran s'affiche demandant si vous souhaitez définir une passerelle principale (routeur par défaut).
A la liste des passerelles de sauvegarde	La machine Firewall_ <nom du modem>_peer est ajoutée parmi les passerelles secondaires.
Ne pas ajouter (configurer plus tard)	Le modem n'est pas défini en tant que passerelle.

Suppression d'un modem

Pour supprimer un modem, sélectionnez-le dans l'arborescence des interfaces, puis cliquez sur le bouton **Supprimer** de la barre d'outils. Le message « Voulez-vous réellement supprimer cette interface ? » s'affiche.
Confirmez ou non votre suppression.
En confirmant la suppression, une vérification de l'utilisation de l'interface (check) est faite.

Remarques générales sur la configuration d'un modem

Le firewall négocie automatiquement l'ouverture de ligne et réinitialise la connexion en cas de coupure. Dans le cas où la connexion n'est pas possible (problème de ligne), le firewall envoie un message d'alarme.

LICENCE

L'écran de Licence se décompose en plusieurs parties :

- L'onglet `Général` : installation manuelle ou automatique d'une licence et consultation des principales informations.
- L'onglet `Détails de la licence` (ou indication du n° de série type `Licence Locale U70XXADA913500` pour différencier le firewall actif d'un firewall passif) : détail de toutes les options de la licence et de leur valeur active sur le firewall.
- Un onglet supplémentaire par boîtier passif dans le cadre de la Haute Disponibilité.

L'onglet « Général »

Cet onglet vous permet d'installer une licence de manière automatique ou manuelle.
Il existe 2 manières d'installer une licence en manuel :

1) En injectant le **Fichier de licence** dans le champ adapté. Possibilité de configurer en automatique.
2) En recherchant une nouvelle licence.

Les boutons

Rechercher une nouvelle licence : Ce bouton sert à la recherche d'une nouvelle licence ou actualise la date de dernière vérification de licence.
En cliquant sur ce bouton, une demande de recherche de licence est faite au boîtier. Si une licence est trouvée, une notification s'affiche au niveau des informations de l'onglet `Général` et l'utilisateur a alors accès au bouton **Installer la nouvelle licence**. La recherche de licence se fait manuellement. Si vous souhaitez une recherche de licence automatique, dans ce cas, il faudra paramétrer la configuration avancée dans cet onglet.
Installer la nouvelle licence : Si le firewall a trouvé une licence par le biais du bouton **Rechercher une nouvelle licence**, le bouton **Installer la nouvelle licence** apparaît en clair. En cliquant dessus, un téléchargement est réalisé. Puis il suffit de confirmer ou non ce téléchargement.

Les dates

Date locale sur le firewall : cette date permet de confirmer que le firewall est à la bonne date. Les dates d'expirations sont calculées selon la date indiquée ici.
Dernière vérification d'une mise à jour de licence effectuée le : dernière date à laquelle une demande de recherche de licence a été faite manuellement ou automatiquement.
Le firewall NETASQ est livré par défaut avec l'ensemble de ses fonctionnalités. Cependant, certaines fonctionnalités (filtrage URL, Haute Disponibilité...) sont optionnelles et ne sont pas activées. D'autres part certaines options, comme la mise à jour, sont limitées dans le temps. Si la date d'expiration est dépassée, certaines options sont désactivées sur le firewall.

Les informations importantes sur la licence

L’écran de configuration de la licence vous donne la version de votre firewall, des informations sur le matériel et les différentes options avec leur date d'expiration s'il y en a une.
Des icônes et des couleurs vous indiquent si une option est proche de l’expiration ou expirée.

Installation à partir d’un fichier

Ici, vous pouvez installer votre première licence si vous n’avez pas d’accès à Internet où si vous souhaitez gérer les licences vous-même.
Si vous choisissez d'utiliser de nouvelles fonctionnalités ou renouveler certaines options, veuillez contacter votre revendeur. Un nouveau fichier chiffré sera alors disponible dans votre espace privé, sur le site Web de NETASQ.

Fichier de licence	Ce champ vous permet d’insérer votre licence préalablement récupérée sur le site web NETASQ et ainsi activer la configuration de votre firewall. Le bouton **Installer le fichier de licence** valide l’installation du fichier de licence sur le boîtier. Les informations concernant votre firewall sont modifiées et les nouvelles options sont activées sur le firewall.



REMARQUE
Certaines options nécessitent un redémarrage.

Configuration avancée

Ici, vous définissez la fréquence de recherche de mise à jour ainsi que le type d’installation (manuelle ou automatique).

Rechercher les mises à jour de licence	Indication de la fréquence de recherche. Si une licence est trouvée, dans ce cas une notification est indiquée dans le panneau d’informations de l’onglet `Général`, de type « ! Une nouvelle licence est disponible pour U30XXA32100950 ».
Installation de la licence après téléchargement	Si vous sélectionnez **toujours manuelle** (via le bouton **« installer une nouvelle licence »**), le bouton **Installer la nouvelle licence** s’affiche dès qu’une licence est proposée. Il est alors possible de comparer la nouvelle licence avec la licence actuelle dans l’onglet `Détails de la licence`. Si la licence vous convient, il suffit de cliquer sur **Installer la nouvelle licence**. Un message de notification s’affiche en vous indiquant que la licence actuelle est à jour. Si vous sélectionnez **automatique lorsque c’est possible (pas de redémarrage requis)**, le boîtier installe la licence. Note : Il existe différents messages de notification : « *Licence Update : une nouvelle licence est disponible* » sera affiché, lorsque tel sera explicitement le cas. Chaque message est associé à une alarme (ici *68*). Il est également possible de trouver : *69= « Licence Update: Licence temporaire, enregistrement nécessaire* » ou encore *71= « Licence Update: Une nouvelle licence a été installée »* Ces messages sont visibles dans les alertes SNMP, syslog, le RealTime Monitor ainsi que les journaux du NETASQ Event Analyzer. Afin d’activer l’envoi de ces messages, vous pouvez vous rendre dans le menu `Notifications`, Ecran `Traces-Syslog` ou `Agent SNMP`.

L'onglet « Détails de la licence»

Cet onglet affiche la licence en vigueur du boîtier sur lequel vous êtes connecté.

Les boutons

Rechercher une nouvelle licence	Ce bouton sert à la recherche d'une nouvelle licence ou actualise la date de dernière vérification de licence. **NOTE** Dans cet onglet, le bouton permet une recherche de licence de tous les firewalls du cluster HA.
Installer la nouvelle licence	Si le firewall a trouvé une licence par le biais du bouton **Rechercher une nouvelle licence**, le bouton **Installer la nouvelle licence** apparaît en clair. En cliquant dessus, un téléchargement est réalisé. Puis il suffit de confirmer ou non ce téléchargement. **NOTE** Dans cet onglet, le bouton permet l'installation de la licence pour le firewall indiqué.
Tout fermer	Rétracte l'arborescence des fonctionnalités de la licence.
Tout dérouler	Déploie l'arborescence des fonctionnalités de la licence.

La grille

Fonctionnalité	Indication des fonctionnalités et des options de chaque fonctionnalité que propose le firewall. Les fonctionnalités sont : « Administration », « Date », « Flags », « Global », « Hardware », « Limit », « Network », « Proxy », « Service », « VPN ». Ci-dessous sont détaillées les options liées aux fonctionnalités.
En cours (licence actuelle)	Indication, pour la licence installée, de l'activation ou non des options pour chaque fonctionnalité, ou de l'état d'expiration. Un symbole explicite indique l'activation de la fonctionnalité, un autre symbole la désactivation d'une option. Des symboles et couleurs font la différence entre une option bientôt expirée (moins de 90 jours de la date d'expiration), une option expirée et une option en cours de validité.
Nouvelle licence	Cette colonne ne s'affiche que si une nouvelle licence est disponible mais pas encore installée, et qu'un redémarrage est nécessaire (en d'autres termes, cette colonne ne s'affichera jamais si vous avez coché dans la configuration avancée de l'onglet `Général` l'option **Installation de la licence après téléchargement automatique lorsque c'est possible (pas de redémarrage requis)**. Lorsqu'une nouvelle licence est disponible, cette colonne présente les nouvelles valeurs en comparaison des valeurs de la licence actuelle indiquées dans la colonne « En cours (licence actuelle)». Des symboles et des couleurs indiquent une amélioration de valeur par rapport à la valeur de la licence actuelle ou une régression. Si l'option n'a pas changé, rien n'est indiqué.

Administration

GlobalAdmin	Administration globale possible via le GlobalAdmin. (Valeur par défaut : 1)
Manager	Administration possible via l'interface Web. (Valeur par défaut : 1).
Monitor	Monitoring possible via NETASQ REALTIME MONITOR (Valeur par défaut : 1).
Reporter	Reporting possible via NETASQ EVENT REPORTER. (Valeur par défaut: 1).

Date

Antispam	Date limite de mise à jour des bases de spams DNSBL.
Antivirus	Date limite de mise à jour des bases virales ClamAV.
ExpressWarranty	Date limite pour l'ExpressWarranty. Cela permet de limiter l'attente du client dans la réparation de son produit.
NotAfter	Date d'expiration de la licence.
NotBefore	Date minimale d'utilisation de la licence
Pattern	Date limite de mise à jour des patterns ASQ.
SPAMVendor	Date limite de mise à jour du moteur heuristique de filtrage des spams.
URLFiltering	Date limite de mise à jour des bases de filtrage d'URL NETASQ.
URLVendor	Date limite de mise à jour des bases de filtrage d'URL OPTENET.
Update	Date limite de mise à jour du boîtier.
VirusVendor	Date limite de mise à jour des bases virales Kaspersky.
VulnBase	Date limite de mise à jour des vulnérabilités SEISMO.
Warranty	Date limite pour la garantie.

Flags

Clone	Active ou désactive la gestion/présence de la partition de backup. (Valeur par défaut : 1).
CustomPattern	Permet la personnalisation des modèles ASQ.
ExpressWarranty	Garantie express qui permet de limiter l'attente du client dans la réparation de son produit.
ExternalLDAP	Active ou désactive l'utilisation d'un annuaire LDAP (Valeur par défaut : 1*)
HAState	Permet de définir un boîtier maître et un esclave dans un cluster HA. (Master/Slave/None).
PKI	Active ou désactive la PKI interne. (Valeur par défaut : 1)
PVS	Active ou désactive SEISMO. (Valeur par défaut : 0)

Global

Comment	Commentaire.
Id	Identifiant unique.
Temporary	Licence temporaire (tant que le boîtier n'a pas été enregistré) ou non. Valeur par défaut : 1 (en sortie d'usine), 0 une fois le produit enregistré.
Version	Version de la licence (vérifie la compatibilité format de licence/version du Firmware). La valeur par défaut est 9.

Hardware

CryptCard	Présence d'une carte optionnelle de cryptographie. (Valeur par défaut : dépend du modèle).
Networkif	Nombre maximum d'interfaces physiques. (Valeur par défaut : dépond du modèle).
Raid	Permet d'acheminer les données d'un disque dur à un autre lorsque l'un d'entre eux tombe.

Limit

Conn	Nombre maximum de connexions passant par l'ASQ. (Valeur par défaut : 0 (= pas de limite)).
Network	Nombre maximum de réseaux gérés par l'ASQ. (Valeur par défaut : 0 (= pas de limite)).
User	Nombre maximum d'utilisateurs qui peuvent s'authentifier sur le boîtier. (Valeur par défaut : 0 (= pas de limite)).

Network

HADialup	Active ou désactive la possibilité d'utiliser les dialups pour réaliser le/les lien(s) HA. (Valeur par défaut : 1).
HybridMode	Active ou désactive le mode hybride des interfaces (mélange d'interfaces, de bridges, de VLANs,…). (Valeur par défaut : 1*).
InterfaceRoute	Permet de faire du routage par interface. Cette option est activée par défaut. Voir le Menu : `Configuration→Réseau→Interfaces/onglet Configuration avancée/ champ Bridge : routage par interface»` (Valeur par défaut : 1).
LBDialup	Active ou désactive le load-balancing sur les dialups. (Valeur par défaut : 1).
QoS	Active ou désactive la QoS. (Valeur par défaut : 1).
VLAN	Active ou désactive les VLANs (Valeur par défaut : 1).

Proxy

Antispam	Active ou désactive le filtrage des spams via DNSBL dans le proxy. (Valeur par défaut : 1).
Antivirus	Active ou désactive l'antivirus ClamaV dans le proxy. (Valeur par défaut : 1).
FTPProxy	Active ou désactive le proxy FTP. (Valeur par défaut : 1**).
HTTPProxy	Active ou désactive le proxy http (Valeur par défaut : 1).
ICAPURL	Active ou désactive l'ICAP ReqMod. (Valeur par défaut : 1).
ICAPVirus	Active ou désactive l'ICAP RespMod. (Valeur par défaut : 1).
IMAPProxy	Active ou désactive le proxy IMAP (qui n'existe pas sur les UTM). (Valeur par défaut : 1).
POP3Proxy	Active ou désactive le proxy POP3. (Valeur par défaut : 1).
SMTPProxy	Active ou désactive le proxy SMTP. (Valeur par défaut : 1).
SpamVendor	Active ou désactive le moteur heuristique de filtrage des spams. (Valeur par défaut : 0).
URLFiltering	Active ou désactive le filtrage d'URL via la base NETASQ dans le proxy. (Valeur par défaut : 1).
URLVendor	Active ou désactive le filtrage d'URL via la base Optenet dans le proxy. (Valeur par défaut : 0).
VirusVendor	Active ou désactive l'antivirus Kaspersky dans le proxy. (Valeur par défaut : 0).

Service

Authentication	Active ou désactive l'interface d'authentification utilisateur.
DHCP	Active ou désactive le service DHCP serveur/relai (Valeur par défaut : 1).
DNS	Active ou désactive le service DNS cache. (Valeur par défaut : 1).
DynDNS	Active ou désactive le client DynDNS de mise à jour de serveur DNS.
Enrolment	Active ou désactive l'enrôlement. (Valeur par défaut : 1).
LDAPBase	Active ou désactive la base LDAP interne (Valeur par défaut : 1).
NTP	Active ou désactive la synchronisation de temps NTP (Valeur par défaut : 1).
PublicLDAP	Active ou désactive l'accès public au LDAP interne (Valeur par défaut : 1*).
SNMP	Active ou désactive l'agent SNMP. (Valeur par défaut : 1*).

Vpn

Anonymous	Active ou désactive la possibilité de monter des tunnels anonymes. (Valeur par défaut : 1*).
PPTP	Active ou désactive les tunnels PPTP. (Valeur par défaut : 1*).
SSL	Active ou désactive le VPN SSL.
StrongEnc	Active ou désactive le support d'algorithmes forts pour l'encryptage dans les tunnels IPSec. (Valeur par défaut : 1*).
Tunnels	Nombre maximal de tunnels IPSec. (Valeur par défaut : 0 (=pas de limite)).

Le fonctionnement de cet onglet est identique à celui de la licence locale.

MANAGEMENT DES VULNERABILITES

Ce menu vous permet de configurer votre politique de management des vulnérabilités susceptibles d'apparaître sur votre réseau.
Vous pouvez assigner un profil de supervision à une machine, un réseau, un groupe ou une plage d'adresses. Il en existe 12 préconfigurés par défaut.

La configuration du management des vulnérabilités consiste donc simplement à :

- Effectuer le lien entre objets réseaux et profils de supervision,
- Décider des destinataires qui recevront les rapports de vulnérabilités.

L'écran de configuration de **Management des vulnérabilités** se divise en 2 zones :

- Une zone de **Configuration générale** : elle comporte une case d'activation du module et des éléments de configuration générale.
- **Configuration avancée :** une zone pour déterminer la durée de vie d'une information et pour les objets exclus.

Configuration générale

Activer la détection d'applications et de vulnérabilités	En cochant cette option, la détection des vulnérabilités est activée et les informations seront visibles notamment depuis le NETASQ REALTIME MONITOR.  **REMARQUE** Lors de la mise à jour (et si vous avez acquis la licence), le module `Management de Vulnérabilités` sera activé par défaut. La remontée d'alertes se fera en fonction de la configuration par défaut : surveiller l'ensemble des vulnérabilités pour toutes les machines internes.  **AVERTISSEMENT** Pensez à mettre à jour la base de vulnérabilités dans `Système\Active Update`. Sans une base à jour, le service ne peut fonctionner correctement. La détection des vulnérabilités repose sur l'analyse du trafic réseau. Cela permet de détecter une application et/ou une faille, dès la première activité de l'utilisateur.
Envoyer les rapports simples à	Groupe de mails à qui seront envoyés des rapports synthétiques. Ces rapports sont succincts et comportent un résumé des vulnérabilités par produit et des machines affectées.
Envoyer les rapports détaillés à	Groupe de mails à qui seront envoyés les rapports complets. Les rapports détaillés comportent un résumé des vulnérabilités, ainsi que leur description détaillée (famille, client, possibilité d'exploitation à distance), ainsi qu'un lien vers sa référence dans la base de connaissance NETASQ, qui inclut généralement des indications sur le correctif à appliquer.

 **REMARQUE**
Les groupes de mails se configurent le menu : `Notifications\Alertes e-mail`\onglet `Destinataires`.

Liste des éléments réseaux sous surveillance

Dans la grille, se trouve la liste des objets surveillés avec le profil de supervision qui leur est associé.

Elément réseau (machine ou groupe – réseau – plage d'adresses)	Choix de l'objet réseau pour lequel s'applique la surveillance. Cet objet est analysé par le moteur NETASQ Vulnerability Manager qui se basera sur les règles contenues dans le profil de supervision associé. L'objet lié au profil ne peut être qu'une machine, un groupe de machines, un réseau ou une plage d'adresses.  AVERTISSEMENT La liste des éléments surveillés est prise en compte de manière ordonnée. Cela signifie que si un élément réseau est présent plusieurs fois dans cette liste, seul le premier profil de supervision s'appliquera.  REMARQUE Il est possible de créer un objet au sein de la colonne à l'aide du bouton
Profil de supervision	Permet de choisir un profil pour restreindre les applications à surveiller. La sélection du profil se fait dans la liste déroulante de la colonne, qui s'affiche en cliquant sur la flèche de droite, lorsque vous ajoutez une ligne au tableau. (voir bouton **Ajouter** ci-dessous)

Vous pouvez réaliser différentes actions à partir de cette grille :

Ajouter	Ce bouton permet d'ajouter un objet réseau et un profil associé à cet objet à la liste des éléments supervisés. En cliquant sur ce bouton, une ligne vide s'affiche dans le tableau.
Supprimer	Sélectionnez l'association objet –profils à supprimer puis cliquez sur le bouton.  AVERTISSEMENT Aucun message ne vous demande de confirmer la suppression du profil.
Monter	Permet d'élever la priorité de l'association entre un élément réseau et un profil.
Descendre	Permet de réduire la priorité de l'association entre un élément réseau et un profil.

Voici la liste des profils et des familles de vulnérabilités qui vont être détectés et signalés :

SERVEURS	APPLICATIONS CLIENTES ET SYSTEMES D'EXPLOITATION	CLIENTS	OUTILS
Serveurs : Serveurs SSH – Serveurs HTTP / Web – Serveurs de Bases de Données – Serveur FTP – Serveurs Mail et Systèmes d'Exploitations **Serveurs - failles critiques** : SSH-Web-Apps-DB-DNS-Web Server-FTP Server-Misc-Mail Server-P2P-OS	**Applications clientes et systèmes d'exploitation (OS)** **Applications clientes et des systèmes d'exploitation (OS) – failles critiques**	**Client mail** : Client, Mail (Thunderbird, Outlook, e-mail …)	**Outils de sécurité** : Antivirus, Outils de Sécurisation et Scanner de vulnérabilités ou de réseaux

Serveurs FTP		**Navigateurs et autres clients web** : Clients web, lecteurs de flux RSS	**Outils d'administration** : Client d'administration FTP, SSH etc.
Serveurs de mail			
Serveurs web : serveurs de contenu web/HTTP			
Serveurs base de données (SQL)			

Le profil « Toutes les applications connues »

Il permet d'attribuer à un objet (machine, groupe, réseau ou plage d'adresses), la détection de toutes les vulnérabilités clientes / serveurs et systèmes d'exploitation détectées par NETASQ Vulnerability Manager.

Configuration avancée

Durée de vie d'une information (jours) [1 – 30] : Durée de rétention de l'information (application, vulnérabilité) sans trafic ou sans mise à jour détecté.

Liste d'exclusion (éléments non supervisés)

Elément surveillé (machine ou groupe – réseau – plage d'adresses)	Une fois les objets associés à un profil, il est possible d'exclure un ou plusieurs objet(s) de l'analyse. Ainsi, quelle que soit la configuration des éléments supervisés, les membres de cette liste d'exclusion ne seront pas surveillés. Le choix des objets à exclure s'effectue à partir de cette grille en cliquant sur le bouton **Ajouter**.

MAINTENANCE

Le module `Maintenance` va vous permettre d'effectuer les réglages et les contrôles de vérification nécessaires au bon fonctionnement de votre équipement.
Via l'interface, il est possible d'établir une configuration sécurisée de votre firewall, de procéder à des sauvegardes et des mises à jour de votre système, comme l'indique les 5 onglets suivants :

- Configuration
- Sauvegarder
- Restaurer
- Configuration sécurisée
- Mise à jour du système

Onglet « Configuration »Disque système

Il est question du disque système de votre firewall multifonction NETASQ.

Vous utilisez actuellement la partition : le disque système de votre firewall est découpé en deux partitions permettant de sauvegarder vos données.
Cette section indique la partition sur laquelle le produit a démarré.
Au démarrage, utiliser la partition : vous allez choisir la partition de démarrage du produit : la partition principale ou de secours.

Partition principale	Si vous cochez cette option, votre firewall utilisera cette partition au démarrage.
Partition de secours	La partition dite de « back up » représente votre dernière partition sauvegardée. Cochez cette option si vous souhaitez l'utiliser au démarrage de votre firewall.
Sauvegarder la partition active	Ce bouton permet de sauvegarder la partition active (celle indiquée par **Vous utilisez actuellement la partition**) sur l'autre partition.

Maintenance

Redémarrer le firewall	Cliquez sur ce bouton pour redémarrer directement votre firewall.
Arrêter le firewall	Cliquez sur ce bouton si vous souhaitez éteindre votre firewall.

Rapport système (sysinfo)

Télécharger le rapport système : Ce bouton va permettre d'obtenir des informations diverses sur votre firewall, au format « sysinfo ».
Par son biais, il est possible de connaître, par exemple, le modèle du firewall, son numéro de série, son état de fonctionnement actuel et l'état sa mémoire.

Onglet « Sauvegarder »

Sauvegarde de configuration

Via cet écran, vous allez pouvoir effectuer une sauvegarde de la configuration de votre firewall sous forme de fichiers, de manière exhaustive, et en protéger l'accès.

Nom donné à la sauvegarde : Par défaut, le nom de la sauvegarde correspondra à « <numéro de série du firewall>_jour_mois_année.na ».

Télécharger	Le fichier sera sauvegardé au format .na (NETASQ ARCHIVES). Cliquez sur ce bouton pour l'enregistrer.

Configuration avancée

Mot de passe	Définissez un mot de passe pour protéger votre sauvegarde.
Confirmer	Confirmez le mot de passe de votre sauvegarde, renseigné dans le champ précédent.
Force du mot de passe	Ce champ indique le niveau de sécurité de votre mot de passe : « Très Faible », « Faible », « Moyen », « Bon » ou « Excellent ». Il est fortement conseillé d'utiliser des combinaisons de lettres minuscules et majuscules, des chiffres ainsi que des caractères spéciaux.

Onglet « Restaurer »

Mot de passe

Cet écran va permettre de restaurer une sauvegarde précédemment effectuée.

Sauvegarde à restaurer :

Sélectionnez un fichier de sauvegarde	Cliquez sur le bouton à droite du champ (…) afin d'insérer le fichier de sauvegarde au format .na à restaurer.
Restaurer la configuration à partir du fichier de sauvegarde	Cliquez ensuite sur ce bouton afin de procéder à la restauration de la configuration du firewall, via le fichier sélectionné ci-dessus. Vous pouvez être amené à redémarrer le firewall selon la sauvegarde restaurée. Si un redémarrage est nécessaire, il est proposé de redémarrer maintenant ou plus tard.

Configuration avancée

Mot de passe de la sauvegarde : Si vous avez protégé la sauvegarde sélectionnée par un mot de passe au sein de l'onglet précédent, `Sauvegarder`, saisissez-le dans ce champ.

Modules à restaurer : il est possible d'effectuer une restauration totale ou partielle de la configuration de votre firewall.

Restaurer tous les modules du fichier de sauvegarde	Cette case est cochée par défaut, si vous choisissez de la maintenir ainsi, l'intégralité des modules contenus dans le fichier de sauvegarde seront restaurés.

Si vous souhaitez ne restaurer qu'une partie des modules du fichier de sauvegarde, décochez la case du dessus afin de dégrisez les champs suivants.
Cochez ceux dont vous souhaitez restaurer la configuration parmi :

- Réseau (Interface, routage et DNS dynamique)
- Filtrage SMTP
- Filtrage URL
- Filtrage SSL
- Objets web
- Modules globaux
- Protection IPS
- Configuration sécurisée
- Active Update
- Services (SNMP, serveur DHCP)
- Profils d'inspection
- Objets réseaux
- Filtrage et NAT
- VPN IPSec
- Annuaire LDAP

Onglet « Configuration sécurisée »

Configuration sécurisée

Cet écran va permettre de protéger l'accès à votre firewall.

Activer le mode de « configuration sécurisée »	Le principe de ce mode est de dissocier « configuration chiffrée » et « clé de déchiffrement » sur deux différents supports : l'une sur une clé USB, l'autre sur le disque dur de votre firewall ; afin que seul l'administrateur en possession de la clé USB ne puisse accéder à la configuration du firewall en le démarrant.
Statut de la clé USB	Ce champ indique l'état de votre clé USB : lorsque le chiffrement de votre sauvegarde a bien été effectué via celle-ci, le champ sera marqué « initialisé ». En tant qu'administrateur, vous pouvez ensuite retirer la clé. Toute personne tentant de redémarrer le boitier sans la clé n'y trouvera qu'une configuration illisible et ne pourra effectuer aucune manipulation. Afin de récupérer la configuration voulue, insérez votre clé USB dans le boitier, démarrez votre firewall, et retirez la une fois le produit opérationnel.

Restauration depuis la clé USB

Restaurer la configuration sur la clé : En insérant votre clé USB dans votre firewall, vous allez pouvoir restaurer le fichier de configuration stocké sur la clé.

Sélectionnez un fichier de sauvegarde	Choisissez le fichier de sauvegarde à récupérer via le bouton [...].
Restaurer la configuration	Cliquez sur ce bouton afin de procéder à la restauration de votre configuration.

Onglet « Mise à jour du système »

Mises à jour disponibles :

Rechercher de nouvelles mises à jour	Le firewall va effectuer une recherche des nouvelles mises à jour du système sur les serveurs update (`Objets/Objets réseaux`) et les affichera à l'écran.

Sélectionnez la mise à jour :

Sélectionnez un fichier .maj	Choisissez la mise à jour du firewall à installer et insérez-là dans le champ à l'aide du bouton [...].
Sauvegarder la partition active sur la partition de sauvegarde avant de mettre à jour le Firewall	En cochant cette option, vous sauvegardez la partition principale de votre système sur la partition de back up, afin d'en conserver une trace. En effet, Le boitier va redémarrer et mettre la version du firewall à jour
Mettre à jour le firewall	Appliquez la mise à jour sélectionnée sur votre boitier en cliquant sur ce bouton.

Configuration avancée

Action

Télécharger le firmware et l'activer	Cette option va permettre d'envoyer le fichier de mise à jour (.maj) et d'activer celui-ci.
Télécharger le nouveau firmware	Cette option permet d'envoyer le fichier de mise à jour sans l'activer. Il est ensuite possible de l'activer via l'option ci-dessous « Activer le firmware précédemment téléchargé ».
Activer le firmware précédemment téléchargé	Si un fichier se trouve sur le firewall, cette option permettra de l'activer. **NOTE** Si un fichier est présent, la version indiquée est présente dans le champ « Mise à jour présente sur le firewall ».

Version actuelle du système

Ce champ affiche la version logicielle actuelle de votre produit.

Mise à jour présente sur le firewall

Ce champ affiche la mise à jour que vous avez sélectionnée préalablement en haut de cet écran.

MESSAGES DE BLOCAGE

L'écran de configuration du module **Messages de blocage** est composé de 2 parties :

- L'onglet **`Antivirus`** : détection d'un virus attaché aux documents, pouvant intervenir au cours de l'envoi et de la réception de mails (POP3, SMTP) ou via le transfert de fichiers (protocole FTP).
- L'onglet **`Page de blocage HTTP`** : page affichée lors d'une tentative d'accès à un site non autorisé par les règles de filtrage.

L'onglet « Antivirus »

Protocole POP3

Contenu de l'e-mail	Ce champ permet de modifier le texte du message reçu si un virus est détecté dans un mail. **Exemple :** *Le firewall NETASQ a détecté un virus dans cet e-mail, il a été extrait par l'antivirus intégré, les pièces jointes infectées ont été supprimées.*

Protocole SMTP

Code d'erreur SMTP	Limité à 3 chiffres, ce champ permet de définir le code d'erreur que le serveur SMTP recevra si un virus est détecté dans un mail envoyé. **Exemple :** *554*
Message associé	Ce champ contient le message informationnel qui sera envoyé au serveur SMTP en cas de détection d'un virus. **Exemple :** *5.7.1 Virus détecté*.

Protocole FTP

Code d'erreur FTP	Limité à 3 chiffres, ce champ contient le code d'erreur que l'utilisateur ou le serveur FTP recevra si un virus est détecté dans un fichier transféré. **Exemple :** *425*
Message associé	Cet emplacement est réservé au message informationnel qui sera envoyé avec le code d'erreur lors de la détection d'un virus au sein de l'envoi/de la réception d'un fichier vers/depuis un serveur FTP. **Exemple :** *Virus détecté. Transfert interrompu.*

L'onglet « Page de blocage HTTP »

Cette fenêtre affiche par défaut la page de blocage HTTP lors d'une tentative d'accès à un site bloqué par les règles de filtrage URL.
La page de blocage par défaut se compose d'une icône et d'une phrase explicite permettant de comprendre pourquoi la page est bloquée, et de savoir à quelle catégorie de groupe d'url obéit le site web non autorisé. Celle-ci étant modifiable dans tous ses aspects, il est possible, par exemple, de faire figurer une icône ou une phrase seule, ou les deux, etc.
Exemple :
Cette page n'est pas autorisée par la politique de la société. Elle fait partie de la catégorie : « Jeux ».

Modifier	Ce bouton permet de personnaliser la page de blocage HTTP en modifiant le code HTML. En cliquant sur ce bouton, une feuille dédiée apparaît en dessous de la fenêtre de blocage par défaut. Cette feuille permet par exemple de changer l'icône d'illustration, le texte, sa police, sa couleur, sa taille.

REMARQUE
Il existe des variables permettant de rendre dynamique les catégories auxquelles appartiennent les sites bloqués :

- $rule : nom de la catégorie.
- $host : le nom du destinataire HTTP (ex : www.google.com).
- $url : URL qui est bloquée.

OBJETS RESEAUX

Ce module est divisé en deux parties :

- La barre d'actions en haut, permettant de trier et de manipuler les objets.
- Deux colonnes dédiées aux objets : l'une les listant, et l'autre affichant leurs propriétés.

La barre d'actions

Rechercher	Si vous recherchez un objet en particulier, saisissez son nom. Le champ de recherche vous permet de lister tous les objets réseaux dont les propriétés correspondent au(x) mot(s) ou lettre(s) clef(s) saisie(s). **Exemple** Si vous saisissez la lettre « a » dans la barre de recherche, la liste en dessous fera apparaître tous objets possédant un « a » dans leur nom ou dans leur description. Vous pouvez également affiner la recherche en fonction du « filtre » listant les différents types d'objets (voir bouton « Filtre » ci-après).  **NOTE** L'icône croix dans le champ de recherche permet de supprimer la saisie et lister tous les objets en fonction du filtre courant. ***A partir de la version 9.0.1***, lorsque vous vous rendez au sein de l'onglet « Objets » dans l'arborescence de gauche, le focus est désormais directement placé dans le champ dédié à la recherche.
Ajouter	Lorsque vous cliquez sur ce bouton, une boîte de dialogue s'affiche et vous propose de créer un objet, en indiquant son type et les informations lui étant relatives dans les champs appropriés.  **REMARQUE** L'objet peut être défini comme « global » au moment de sa création si vous cochez l'option « *Cet objet est global* » au sein de la boîte de dialogue. Il apparaîtra lorsque vous opterez pour le filtre « Tous les objets » ou « Réseau » (voir ci-dessous) et sera matérialisé par l'icône suivante.
Supprimer	Sélectionnez l'objet à retirer de la liste et cliquez sur **Supprimer**.
Vérifier l'utilisation	Si vous cliquez sur ce bouton après avoir sélectionné un événement, le résultat s'affiche dans l'arborescence des modules.

Le filtre

Ce bouton permet de choisir le type d'objets à afficher. Un menu déroulant vous propose les choix suivants :

Tous les objets	Matérialisée par l'icône , cette option permet d'afficher dans la liste des objets à gauche, tous les types d'objets réseaux.
Machine	Matérialisée par l'icône , cette option permet d'afficher uniquement les

	objets de type « machine » dans la colonne de gauche.
Réseau	Matérialisée par l'icône, cette option permet d'afficher uniquement les objets de type réseaux.
Plage d'adresses IP	Matérialisée par l'icône, cette option permet d'afficher uniquement les plages d'adresses IP.
Port – plage de ports	Matérialisée par l'icône , cette option permet d'afficher les ports et les plages de ports.
Protocole IP	Matérialisée par l'icône , cette option permet d'afficher uniquement les protocoles IP.
Groupe	Matérialisée par l'icône, cette option permet d'afficher uniquement les groupes de réseaux.
Groupe de ports	Matérialisée par l'icône, cette option permet d'afficher uniquement les groupes de ports.

Les différents types d'objets

Machine

Sélectionnez une machine pour visualiser ou éditer ses propriétés. Chacune d'entre elles possèdent par défaut un nom, une IP et une résolution DNS (« Automatique » ou « Aucune (IP statique »).

Nom de l'objet	Nom donné à l'objet lors de sa création. Ce champ est modifiable, il faudra cliquer sur « **Appliquer »** et « **Sauvegarder** » pour enregistrer le changement. ***A partir de la version 9.0.1,*** l'icône à droite de la case permet d'obtenir l'IP de l'objet, visible au sein du champ « Adresse IP ». Pour cela, il faut avoir saisi l'url complète de l'objet.
Commentaire	Description associée à la machine sélectionnée.
Résolution DNS	La résolution DNS (*Domain Name System*) associe des adresses IP et un nom de domaine. Deux choix sont possibles : Une IP **Automatique** (ou dites « dynamique ») : Si vous cochez cette case, l'objet sélectionné recevra une adresse IP périodiquement. **Aucune (IP statique)** : L'objet sélectionné possède une adresse IP fixe qui sera utilisé systématiquement.
Adresse IP	Adresse IP de la machine sélectionnée.
Adresse MAC	*Media Access control adress*. Elle correspond à l'adresse physique d'une interface réseau ou d'une carte réseau, permettant d'identifier une machine sur un réseau local. **Exemple** *5E:FF:56:A2:AF:15.*

Réseau

Sélectionnez un réseau pour visualiser ou éditer ses propriétés. Ils possèdent chacun un nom, une IP et un masque réseau.

Nom de l'objet	Nom donné à l'objet lors de sa création. Ce champ est modifiable, il faudra cliquer sur « **Appliquer »** ou « **Sauvegarder** » pour enregistrer le changement.
Commentaire	Description associée au réseau sélectionné.
Adresse IP	Adresse IP du réseau sélectionné.
Masque de réseau	Masque de réseau ou de sous-réseau.

Plage d'adresses IP

Sélectionnez une plage d'adresses IP pour visualiser ou éditer ses propriétés.

Nom de l'objet	Nom donné à l'objet lors de sa création. Ce champ est modifiable, il faudra cliquer sur « **Appliquer »** ou « **Sauvegarder** » pour enregistrer le changement.
Commentaire	Description associée à la plage d'adresses IP sélectionnée.
Début	Première adresse IP associée à la plage.
Fin	Dernière adresse IP associée à la plage.

Port – plage de ports

Sélectionnez un port ou une plage de ports pour visualiser ou éditer ses propriétés.

Nom de l'objet	Nom du service utilisé. Ce champ est grisé et non modifiable.
Commentaire	Description associée au port ou à la plage de ports sélectionnés.
Port	Numéro du port associé au service sélectionné.
Plage de port	En cochant cette case, vous attribuerez une plage de port au service sélectionné et dégrisez la case du dessous.
Fin de la plage	Si la case précédente est cochée, ce champ est dégrisé et la fin de la plage correspond au chiffre ou au nombre suivant du port sélectionné. **Exemple** Si vous choisissez l'objet « cmd » figurant sur le port « 514 », la fin de plage sera notée « 515 ».
TCP/UDP	Choisissez le protocole IP utilisé par votre service : **TCP** : *Transmission Control Protocol*. Protocole de transport fonctionnant en mode connecté et composé de trois phases : l'établissement de la connexion, le transfert des données, la fin de la connexion. **UDP :** *User Datagram Protocol.* Ce protocole permet de transmettre les données de manière simple entre deux entités, chacune étant définie par une adresse IP et un numéro de port. **Tout protocole** : N'importe quel protocole IP pourra être utilisé par le service sélectionné (TCP, UDP ou autre).

Protocole IP

Nom de l'objet	Nom du protocole IP sélectionné. Ce champ est grisé et non modifiable.
Commentaire	Description associée au protocole IP sélectionné.
Numéro du protocole	Nombre ou chiffre associé au protocole IP sélectionné.

Groupe

Cet écran va vous permettre d'agréger vos objets selon votre topologie réseau, par exemple.

Nom de l'objet	Nom donné au groupe d'objets lors de sa création. Les objets en « lecture seule » seront grisés et ne pourront pas être modifiés.
Commentaire	Description associée au groupe d'objets.
Editer ce groupe	Ce bouton comporte une boîte de dialogue d'ajout d'objet(s) au sein du groupe. Deux colonnes apparaissent : Celle de gauche comporte la liste de tous les objets réseaux que vous pouvez ajouter à votre groupe. La colonne de droite comporte les objets qui figurent déjà dans le groupe. Pour ajouter un objet dans le groupe, vous devrez le faire passer d'une colonne à une autre : 1 Sélectionnez le ou les éléments à ajouter. 2 Cliquez sur cette flèche-ci ➡, l'objet bascule dans la colonne de droite et intègre votre groupe (en tête de la liste). Pour retirer un objet du groupe, sélectionnez-le dans la colonne de droite et cliquez sur cette flèche ⬅. **NOTE** En cliquant sur le bouton « Editer ce groupe », vous pouvez, d'une part, changez le nom du groupe et lui attribuer un commentaire, et d'autre part, effectuer une recherche d'objet(s) et en inclure de nouveaux au sein du groupe.
Objets dans ce groupe	Vous visualisez les objets réseaux figurant dans votre groupe au sein d'un tableau. Pour tout ajout ou modification, reportez-vous au champ précédent.

Groupe de ports

Cet écran va vous permettre d'agréger vos ports par catégorie.
Exemple
Un groupe « **mail** » regroupant les ports « imap », « pop3 » et « smtp ».

Nom de l'objet	Nom donné au groupe de ports lors de sa création.
Commentaire	Description associée au groupe de ports.
Editer ce groupe	Ce bouton comporte une boite de dialogue permettant d'ajouter des port(s) au sein du groupe. Lorsque vous cliquez dessus, vous pouvez, d'une part, changer le nom du groupe et

	lui attribuer un commentaire, et d'autre part, effectuer une recherche de port(s) et en inclure de nouveaux au sein du groupe. Deux colonnes apparaissent : Celle de gauche comporte la liste de tous les ports que vous pouvez ajouter à votre groupe. La colonne de droite comporte les ports qui figurent déjà dans le groupe. Pour ajouter un port dans le groupe, vous devrez le faire passer d'une colonne à une autre : 1 Sélectionnez le ou les éléments à ajouter. 2 Cliquez sur cette flèche-ci, l'objet bascule dans la colonne de droite et intègre votre port (en tête de la liste). Pour retirer un objet du groupe, sélectionnez-le dans la colonne de droite et cliquez sur cette flèche .  **NOTE** En cliquant sur le bouton « Editer ce groupe », vous pouvez, d'une part, changez le nom du groupe et lui attribuer un commentaire, et d'autre part, effectuer une recherche d'objet(s) et en inclure de nouveaux au sein du groupe.
Objet dans ce groupe	Vous visualisez les ports figurant dans votre groupe au sein d'un tableau. Pour tout ajout ou modification, reportez-vous au champ précédent.

OBJETS TEMPS

Le module `Objets Temps` se compose de deux écrans :

- A gauche : une zone réservée à la création des Objets Temps.
- A droite : une zone affichant les détails concernant les objets créés.

Les actions

Ajouter	Vous pouvez créer deux types d'objets temps : **Ajouter un événement ponctuel** : Ce type d'événement est limité dans le temps, il a une date de début et une date de fin. Il sera nommé « **événement_ponctuel »** au sein de la liste avant de se voir attribuer un autre nom. **Ajouter un événement périodique** : Ce type d'événement n'est pas limité dans le temps, il peut survenir chaque jour, et posséder une plage horaire. Aucune date de fin n'est précisée. Il sera nommé « **événement_récurrent** » au sein de la liste avant de se voir attribuer un autre nom.
Supprimer	Sélectionnez l'événement à retirer de la liste et cliquez sur **Supprimer**.
Vérifier l'utilisation	Si vous cliquez sur ce bouton après avoir sélectionné un événement, le résultat s'affiche dans l'arborescence des modules. Vous pouvez également retrouvez les objets temps existants en vous rendant dans la zone « Objets » de l'arborescence des modules et vous rendre soit, dans la barre de recherche par mots clés pour le retrouver, soit en cliquant sur l'icône et sélectionnez « Objets temps » via la liste déroulante affichée.
Dupliquer	Positionnez-vous sur un objet existant et cliquez sur ce bouton, il sera nommé <nom de l'événement_type d'événement_0).
Nom	Vous ne pouvez pas changer le nom de votre objet au sein de cette colonne. Sélectionnez-le d'abord et utilisez l'écran de droite, dédié aux détails des événements pour le définir (*voir partie suivante*).
Commentaire	Vous ne pouvez effectuer aucune description d'objet au sein de cette colonne. Sélectionnez-le d'abord et utilisez l'écran de droite, dédié aux détails des événements pour le commenter (*voir partie suivante*).
Configuration avancée	Ce bouton permet d'ajouter des options à l'objet temps sélectionné : **Evénement ponctuel** **Jour de l'année** **Jour de la semaine** **Plage horaire** Les options cochées s'afficheront au sein de votre écran de droite.

Les informations concernant les objets

L'événement hebdomadaire est décrit par défaut comme ayant lieu « *du lundi au vendredi. De 9h à 17h*».
L'événement ponctuel est décrit par défaut comme ayant lieu *« Du <date> au <date> à <heure>. Toutes les semaines du lundi au vendredi »* avec précision d'heure.
L'événement annuel est décrit par défaut comme ayant lieu le *1er janvier de 9h à 17h.*

L'événement ponctuel

Ce champ permet de préciser « Depuis » quand l'événement a lieu et jusque quand il se tiendra. Il faut définir un jour au sein du calendrier présenté.
Vous devez également définir une heure en remplissant le champ vide marqué « à ».

Le jour de l'année

Par défaut, ce champ indique la date du 01: 01, vous pouvez cliquez sur **Ajouter une plage de dates** et saisir une date de début et une date de fin pour votre événement, en choisissant le mois et le jour.

Les Jour(s) de la semaine

Les jours concernés par l'événement sont marqués par cette icône . Si vous souhaitez en retirer un, cliquez une fois dessus. Si vous souhaitez en appliquer un supplémentaire, comme le samedi par exemple, cliquez une fois sur la case « Sam ». Celle-ci sera alors marquée par l'icône décrite ci-dessus et ce jour sera concerné par votre événement.

Les plage(s) horaire(s)

Vous pouvez définir la/les Plage(s) horaire(s) à l'aide de ces boutons :

Ajouter une plage horaire, pour ainsi effectuer l'action citée et paramétrer l'heure de début et de clôture de votre événement.

Pour la supprimer.
Les nouvelles informations concernant la/les plage(s) horaire(s) s'afficheront dans le champ **Description**.

OBJETS WEB

Ce module se compose de 3 onglets :

- **URL** : Permet de rassembler les URL par catégorie, en créant des groupes (exemples : « shopping », « pornography », « videogames »). Chacun de ces groupes réunit un certain nombre d'URL de sites web, qui pourront être bloquées, ou autorisées, en fonction de l'action souhaitée.
- **Nom de certificat (CN)** : Permet de reconnaître les certificats attribués aux sites web sécurisés, fonctionnant avec le filtrage SSL, ainsi que de les rassembler par catégorie en créant des groupes.
- **Base d'URL** : Suivant le type de service de maintenance souscrit, les listes d'URL disponibles sont mises à jour par des fournisseurs différents (parmi NETASQ ou OPTENET). Les listes d'URL NETASQ sont proposées par défaut, lorsque le type de service de maintenance souscrit est « standard ».

Onglet « URL »

Il donne une vue d'ensemble des URL classées par catégorie et par groupe.
Pour un groupe donné, par exemple « banks », dans lequel seront rassemblées des URL des banques les plus consultées, il sera possible de créer une règle au sein du `Filtrage URL` (`Politique de Sécurité\Filtrage URL`) pour en interdire l'accès.

Ainsi, lorsque vous tenterez de vous connecter au site web de votre banque, une page de blocage s'affichera, avec un message d'erreur. (Voir le module `Notifications\Messages de blocage\`onglet `Page de blocage HTTP`).

Grille de groupe d'URL

L'écran de groupe d'URL se décompose en 2 parties : une première partie pour les groupes d'URL, une seconde partie pour les URL.

Vous pouvez, au niveau de la configuration des groupes, effectuer les actions suivantes :

Ajouter un groupe d'URL	Crée un nouveau groupe. En cliquant sur ce bouton, une nouvelle ligne s'affiche vous permettant d'indiquer le nom du groupe et un éventuel commentaire.
Supprimer	Supprime un groupe ou une URL existante. Sélectionnez la ligne à supprimer puis cliquez sur ce bouton. Le message suivant s'affiche : « Voulez-vous supprimer le groupe xxx ? ». Si le groupe est utilisé dans ce cas un message vous prévient et vous demande à nouveau ce que vous souhaitez faire.
Vérifier l'utilisation	Permet de vérifier si le groupe sélectionné au préalable est utilisé dans une configuration. Lorsque vous cliquez sur ce bouton, un panneau s'affiche au niveau de l'arborescence des modules et indique les modules qui utilisent ce groupe.

La grille présente les éléments indiqués ci-dessous :

Groupe d'URL	Nom du groupe d'URL.

Commentaire	Description du groupe d'URL.

Format

La description de ce champ est valable pour les URL uniquement. Les groupes d'URL ne sont pas touchés par les restrictions de format.
La saisie d'un masque d'URL peut comporter la syntaxe suivante :

*****	Remplace une séquence de caractères quelconque. **Exemple** *.netasq.com/permet de définir le domaine Internet de la société NETASQ.
?	Remplace un caractère. **Exemple** ???.netasq.com est équivalent à www.netasq.com ou de ftp.netasq.com mais pas à www1.netasq.com.

Un masque d'URL peut contenir une URL complète (**exemple** : www.netasq.com*) ou des mots-clés contenus dans l'URL (**exemple** : *mail*).
Il est aussi possible de filtrer des extensions de fichiers :

Exemple

le masque d'URL '*.exe' peut servir à filtrer les fichiers exécutables.



La description de ce champ est valable pour les URL uniquement. Les groupes d'URL ne sont pas touchés par les restrictions de format.
Néanmoins, le nombre de caractères pour un groupe d'URL est limité à 255 Ko.

Grille d'URL (« Groupe d'URL : All »)

Vous pouvez, au niveau de la configuration des URL de groupes, effectuer les actions suivantes :

Ajouter une URL	Ajoute une URL à un groupe. Sélectionnez d'abord le groupe dans lequel vous voulez ajouter une URL dans la colonne de gauche, puis cliquez sur ce bouton.
Supprimer	Supprime une URL à un groupe. Sélectionnez d'abord le groupe dans lequel vous voulez supprimer une url dans la colonne de gauche, puis cliquez sur ce bouton.

La grille présente les éléments indiqués ci-dessous :

Nom de l'URL	Nom de l'url. Il peut contenir des wilcard.



Il existe deux types de groupes d'URL : des groupes d'URL statiques (entrés manuellement par l'administrateur) et des groupes d'URL dynamiques (Cf. Filtrage d'URL dynamique ci-dessous).
Le fournisseur demandé est le fournisseur des groupes d'URL dynamiques, par défaut NETASQ.

Les groupes d'URL statiques dépendent du choix du fournisseur de filtrage Web.
Si vous choisissez un autre fournisseur, il faut s'assurer que le slot de filtrage URL actif n'utilise pas de groupes URL statiques de l'ancienne liste, sous risque de rendre non valide cette configuration durant et après le changement de fournisseur.

Onglet « Nom de certificat (CN)»

Cet écran contenant des groupes de nom de certificat peut s'avérer utile le filtrage SSL (voir le module `Politique de Sécurité\Filtrage SSL)`. Il est composé de 2 parties : une pour les groupes, une seconde pour les URL.
L'écran se présente de manière similaire à l'onglet **`Groupe d'URL`** hormis que la liste de droite contient des noms d'autorité de certification (CA).



NOTE
Le nombre de caractères pour un groupe de CN est limité à 255 Ko.

Onglet « Base d'URL »

Cet onglet permet de modifier le fournisseur de groupe d'URL/nom de certificat.

Fournisseur de base d'URL	Suivant le type de service de maintenance souscrit (***Voir la politique tarifaire NETASQ en cours***), les listes d'URL disponibles sont mises à jour dynamiquement par des fournisseurs différents (parmi NETASQ ou OPTENET). Par défaut lorsqu'un service de maintenance "standard" est souscrit, ce sont les listes d'URL NETASQ qui sont proposées. Lorsque vous souscrirez au service de maintenance, pour activer la fonctionnalité de filtrage d'URL sur les listes d'URL OPTENET, sélectionnez dans la liste des fournisseurs proposés : OPTENET. En changeant de fournisseur, le message suivant s'affiche : «La base d'URL actuelle **va être supprimée**, puis la base du fournisseur Optenet sera téléchargée. Entre temps, toute politique de filtrage URL qui utilise une catégorie du fournisseur actuel **cessera de fonctionner**. Durant la migration, il est conseillé d'appliquer une politique de filtrage URL qui ne fait pas appel aux catégories d'URL. Êtes-vous sur de vouloir changer de fournisseur ? ». L'Appliance prendra en compte la demande et effectuera le téléchargement des nouvelles listes d'URL grâce au module **Active Update**.

Un encadré situé sous la liste déroulante affiche des informations concernant les groupes d'URL du fournisseur en cours d'utilisation.

PORTAIL D'IDENTIFICATION

Connexion

Pour pouvoir configurer votre firewall NETASQ, il faut vous connecter à l'interface d'administration web.

La configuration d'un firewall n'est accessible qu'aux administrateurs du produit. L'attribution des droits aux utilisateurs et/ou aux groupes d'utilisateurs est effectuée dans le menu `Système\Administrateurs` par le « super admin » ou l'administrateur qui dispose de tous les droits.

Présentation de l'écran

Le module de connexion se décompose en 2 parties :

- Une partie fixe
- Une partie rétractable : options

Les indications à fournir varient selon qu'il s'agit d'une première connexion au firewall ou pas.

Utilisateur	Champ réservé au login utilisateur disposant au minimum des droits base.
Mot de passe	Mot de passe de l'utilisateur, qui sera invité à en saisir un s'il s'agit de sa première connexion. Pour une configuration par défaut, il n'y a pas de mot de passe (champ vide).
S'authentifier en utilisant un certificat SSL	Lorsque cette case est activée, les champs **Utilisateur** et **Mot de passe** ne sont plus nécessaires, donc grisés. Le message suivant s'affiche : *« L'utilisation de certificat vous permet de vous authentifier automatiquement. Voulez-vous activer l'authentification automatique ? »*. Sélectionnez **Authentification automatique** ou **Authentification manuelle**. **REMARQUE** L'option de connexion automatique peut être activée automatiquement dans l'écran des `Préférences\Paramètres de connexion\`*Se connecter automatiquement en utilisant un certificat SSL.*
S'authentifier	Un clic sur ce bouton ou appuyer sur la touche « Entrée » permet d'envoyer les informations de connexion au firewall.



AVERTISSEMENT

Le firewall NETASQ est sensible à la casse, il fait la différence entre les majuscules et les minuscules, aussi bien pour le nom d'utilisateur que pour le mot de passe.

Options

Langue	Langue de l'IHM Web. Lorsque l'utilisateur choisit une nouvelle langue pour l'IHM Web, la page d'authentification se recharge dans la langue choisie. Les langues disponibles sont l'anglais, l'espagnol, le français, l'italien et le polonais.
Lecture seule	Permet une connexion en mode "lecture". Ainsi vous pouvez vous connecter au firewall sans droits de modifications au moyen d'un compte possédant habituellement ces droits. Ceci permet de ne pas utiliser les droits de modifications si cela n'est pas nécessaire.

REMARQUE

- Les options sont contenues dans un cookie. L'utilisateur conserve donc sur son navigateur ses préférences de connexion.
- Si, lors de la connexion sur la page d'authentification, l'option « Lecture seule » se trouve activée dans le cookie, la partie des options sera présentée déployée à l'utilisateur afin d'éviter toute confusion.

Notifications d'erreurs

Lorsqu'un champ est vide

Si l'utilisateur tente de s'authentifier alors qu'il n'a pas renseigné le champ **Utilisateur** ou **Mot de passe**, l'authentification n'est pas lancée et le message « Ce champ doit être renseigné » s'affiche.

Lorsque la touche « Caps lock » est activée

Si cette touche est activée lorsque l'utilisateur renseigne son mot de passe, une icône d'avertissement s'affiche « la touche Verrouillage Majuscule est active ».

Echec d'authentification

Lorsqu'il y a échec d'authentification, le message suivant « *L'authentification a échoué* » s'affiche en rouge.

REMARQUE

Protection contre les attaques par force brute :
Lorsqu'un trop grand nombre de requête est effectué avec un mot de passe incorrect, le message suivant s'affiche : « *La protection de l'authentification contre les attaques par force brute a été activée. La prochaine tentative d'authentification sera possible dans **<nombre de secondes>**.*

Le compte « admin », super administrateur

Par défaut, il n'existe qu'un seul utilisateur possédant des droits d'administration des produits NETASQ, le compte "admin" (son login est "admin"). Cet administrateur possède tous les droits. Il peut effectuer certaines opérations comme modifier la méthode d'authentification d'un utilisateur par exemple.

REMARQUE

Etant donné les droits du compte "admin", NETASQ conseille de n'utiliser ce compte qu'en test ou dans le cas d'une maintenance.

Seul l' « admin » peut attribuer des droits d'administration à d'autres utilisateurs.

Déconnexion

Pour vous déconnecter d'un firewall, suivez la procédure suivante :

1. Sélectionnez en haut à droit de l'interface. L'écran « Quitter ? » s'affiche avec le message suivant « **Vous allez être déconnecté.** ». Cliquez ensuite sur **Quitter**, ou **Annuler** si vous ne souhaitez pas poursuivre la déconnexion.
2. En cliquant sur **Quitter**, L'interface revient à l'écran de connexion. L'annulation provoque le retour à l'écran principal, sans conséquence pour la suite de l'exécution du programme.

PRÉFÉRENCES

Ce module est accessible via le bouton en haut de votre écran IHM.
Il va vous permettre de gérer les paramètres de votre interface web.
Selon vos choix d'options, vous pourrez gagner en ergonomie et en rapidité.

Accès au site web NETASQ

Identifiant	Votre login NETASQ (en général nom.prenom ou votre adresse mail)
Mot de passe	Saisissez votre mot de passe. L'icône vous permet de l'afficher en clair afin d'éviter toute erreur.
Accéder à l'espace personnel NETASQ	Cliquez sur ce bouton pour accéder directement à votre espace sécurisé NETASQ (également accessible sur www.netasq.com).

Paramètres de connexion

Se connecter automatiquement en utilisant un certificat SSL	En cochant cette option, vous n'aurez plus besoin de vous identifier, vous serez directement reconnu grâce à votre certificat SSL.
Déconnexion en cas d'inactivité	Il est possible de fixer un délai pour la déconnexion de votre interface web : 5 minutes 15 minutes 30 minutes 1 heure Vous pouvez également choisir de « Toujours rester connecté ».
A la connexion, afficher systématiquement le dernier module actif	En cochant cette case, à chaque fois que vous vous connecterez, vous serez redirigé sur le dernier module affiché avant la déconnexion.

Paramètres de l'application

Toujours afficher les éléments de configuration avancée	Les éléments de configuration avancée sont déroulables au sein de chaque module en comportant, mais sont masqués par défaut. En cochant cette case, vous les rendrez visibles à l'écran sans avoir besoin de les dérouler.
Afficher les utilisateurs dès l'accès au module	En cochant cette option, tous les utilisateurs seront affichés au sein de l'arborescence de gauche.
Afficher les objets réseaux dès le lancement du module	En cochant cette option, tous les objets réseaux seront affichés au sein de l'arborescence de gauche.
Afficher la politique de sécurité globale (Filtrage et NAT)	En cochant cette case, lors de la connexion au menu `Politique de Sécurité\Filtrage et NAT`, l'écran affichera la politique de sécurité locale en vigueur.
Affichage de la politique de sécurité	Selon le nombre de règles existantes, vous pouvez choisir d'en afficher : 30 règles par page 50 règles par page 100 règles par page 200 règles par page 500 règles par page En choisissant « Automatique », le moteur NETASQ essayera de déduire le nombre de règles par page, en fonction de votre configuration.

Paramètres de l'interface de management

Vérifier tous les champs d'un objet lors d'une recherche	Lorsque vous effectuez une recherche par lettre ou par mot dans les champs dédiés, le moteur va aussi bien vérifier les noms que les commentaires, tout ce qui concerne le sujet de la recherche.
Désactiver les diagnostics en temps réel de la politique de sécurité	Lorsque vous créez une règle au sein de la politique de sécurité, le moteur de diagnostic va automatiquement vérifier si des règles se chevauchent, si des erreurs sont repérées. En cochant cette case, vous suggérerez une recherche manuelle de ces possibles erreurs.
La semaine commence le dimanche	En cochant cette case, les `Objets temps` figurant dans le menu `Objets` démarreront leur semaine le dimanche.
Confirmer avant d'appliquer les modifications	Cette option va permettre d'annuler vos actions si vous avez effectué une fausse manipulation ou si vous décidez de ne pas poursuivre votre configuration. En effet, une fenêtre de confirmation s'affichera, permettant de valider ou non votre action.

Liens externes

URL d'accès à l'aide en ligne	Cette URL vous rappelle l'adresse d'accès à l'aide en ligne NETASQ : vous y trouverez l'arborescence des modules par ordres alphabétique. Cliquez sur le module de votre choix afin d'afficher la page correspondante.
URL d'accès à la documentation des alarmes	Cette adresse vous permettra d'accéder à un document d'aide à la compréhension du module `Alarmes`, figurant dans la base de connaissance NETASQ.
URL d'accès à la suite d'administration	Cette URL vous permet de télécharger la suite d'administration NETASQ soient : Monitor, Reporter, et GlobalAdmin.

PROFILS D'INSPECTION

Le module de profils d'inspection se compose de 2 écrans :

- Une zone dédiée à la configuration par défaut et un menu rétractable pour le mode avancé.
- Une zone de configuration pour l'association des profils protocolaires, accessible via le bouton « **Accéder au profils** ».

Inspection de sécurité

Configuration commune à chaque profil

Configuration par défaut

Configuration pour le trafic entrant	Définissez le profil à appliquer pour le trafic entrant du réseau via le firewall NETASQ. Le trafic entrant représente le trafic d'une interface non protégée (comme Interner) vers une interface protégée (votre réseau local/interne).
Configuration pour le trafic sortant	Définissez le profil à appliquer pour le trafic sortant du réseau via le firewall NETASQ. Le trafic sortant représente le trafic d'une interface protégée vers une interface non protégée.

Nouvelles alarmes

Appliquer le modèle par défaut aux nouvelles alarmes	Cette option est liée au module `Protection Applicative\Alarmes`. En la cochant, les nouvelles alarmes se mettront à jour automatiquement et seront livrées avec la signature NETASQ. Les trois options suivantes seront grisées car vous aurez fait le choix d'une configuration automatique. Si vous souhaitez les appliquer vous-mêmes, décochez la case et définissez les paramètres des champs suivants.
Action	Lorsqu'une alarme est remontée, le paquet qui a provoqué cette alarme subit l'action associée. Vous pouvez choisir de laisser **Passer** ou de **Bloquer** les nouvelles alarmes. Vous pourrez constater l'état que vous avez appliquez au sein du module `Protection Applicative\Alarmes`. Les nouvelles alarmes se trouvent dans la colonne « **Nouveau** ».
Niveau	Trois niveaux d'alarmes sont disponibles, "Ignorer", "Mineur" et "Majeur".
Capture du paquet	En cochant cette option, le paquet responsable de la remontée de l'alarme sera capturé.

Configuration avancée

Appliquer les opérations de translation (NAT) avant le VPN IPSec	Cette option signifie que les adresses IP seront modifiées avant le chiffrement effectué par le VPN IPSec.
Considérer les interfaces IPsec comme interne	Lorsqu'une machine tente d'accéder à une interface protégée via un tunnel VPN IPSec, ses données sont déchiffrées et elle ensuite enregistrée. Elle passera ainsi d'un réseau distant (ou d'un statut d'interface externe) au réseau local (ou au statut d'interface interne).

Configurer les profils

Cet écran se compose de 2 parties :

- Une zone d'édition des différentes configurations de profils possibles
- Une zone d'association des profils protocolaires

Choisissez le profil applicatif associé au protocole en le sélectionnant au sein de la liste déroulante, à l'aide de la flèche à droite du champ.
Pour revenir au menu précédent cliquez sur le bouton « **Accéder à la configuration globale** ».

PROTOCOLES ET APPLICATIONS

Ce module contient la liste des divers protocoles et applications configurables depuis votre interface web.

Il est divisé en 2 zones distinctes :

- Les protocoles (colonne de gauche)
- Les profils attribuables aux protocoles et leur configuration (colonne de droite)

La zone réservée aux profils est vide par défaut, et propose de « Sélectionner un protocole » dans la colonne de gauche.

Les protocoles

Recherche

La barre de recherche permet de retrouver le protocole à configurer en saisissant les premières lettres de son nom. Il est possible de travailler directement avec le protocole voulu en cliquant dessus.

Liste des protocoles

Choisissez le protocole que vous souhaitez paramétrer au sein de la liste affichée.

Une fois le protocole choisi, la configuration de celui-ci peut démarrer.

Les profils

Sélection du profil

Le menu déroulant propose 10 profils, numérotés de 00 à 09.
Chaque profil possède par défaut, le nom « Default », accompagné de sa numérotation.
Exemples :

- (0) Defaut00
- (1) Default01…

Les boutons

Editer	Cette fonction permet d'effectuer 3 actions sur les profils : • **Renommer** : en cliquant sur cette option, une fenêtre composée de deux champs à remplir s'affiche. Celle-ci propose de modifier le nom

	d'une part et d'ajouter un commentaire d'autre part. Une fois l'opération effectuée, cliquez sur « Mis à jour ». Il est également possible d' « annuler » la manipulation. • **Réinitialiser** : Permet de rendre au profil sa configuration initiale, de sorte que toutes les modifications apportées soient supprimées. • **Copier vers** : Cette option permet de copier un profil vers un autre, toutes les informations du profil copié seront transmises au profil récepteur. Il portera également le même nom.
Dernière modification	Cette icône permet de connaître la date et l'heure exactes de la dernière modification effectuée. Si le profil sélectionné possède un commentaire, celui-ci sera affiché au sein d'une info-bulle.
Configurer la partie commune à chaque profil	Cette option contient la liste des ports TCP par défaut. Cette option est présente dans chaque protocole sauf : IP, ICMP, RTP, RTCP. Il est possible d'**Ajouter** ou de **Supprimer** des ports en cliquant sur les boutons du même nom.

HTTP

L'activation de ce protocole permet la prévention de grandes familles d'attaques applicatives basées sur le protocole HTTP. Les différentes analyses effectuées par ce protocole (notamment la vérification de la conformité aux RFC), la validation de l'encodage utilisé dans l'URL ou la vérification de la taille de l'URL et du corps de la requête, vous permettent de stopper des attaques telles que Code RED, Code Blue, NIMDA, HTR, Buffer Overflow ou encore Directory Traversal.

La gestion des débordements de tampons (ou Buffer Overflow) est primordiale chez NETASQ, c'est pourquoi la définition des tailles maximales permises pour les tampons dans le cadre du protocole HTTP est particulièrement développée.

Onglet « IPS »

Détecter et inspecter automatiquement le protocole	Si le protocole est activé, il est automatiquement utilisé à la découverte d'un paquet correspondant dans les règles de filtrage. Cette option n'est pas disponible pour les protocoles, IP, ICMP TCPUDP, RTP, RTCP, MSN, YMSG.

Extensions du protocole HTTP

Autoriser le protocole Shoutcast	Cette option autorise le transport de son à travers le protocole HTTP. **Exemples :** Webradio, webtv.
Autoriser les connexions WebDAV (lecture et écriture)	Cette option permet d'ajouter des fonctionnalités d'écriture et de verrou au protocole HTTP, ainsi que de sécuriser plus facilement les connexions HTTPS.

Commandes HTTP autorisées

Liste des commandes HTTP autorisées (au format CSV). Toutes les commandes incluses ne peuvent excéder 126 caractères.
Il est possible d'**Ajouter** ou de **Supprimer** des commandes via les boutons du même nom.

Commandes HTTP interdites

Liste des commandes HTTP interdites (au format CSV). Toutes les commandes incluses ne peuvent excéder 126 caractères.
Il est possible d'**Ajouter** ou de **Supprimer** des commandes via les boutons du même nom.

URL : taille maximale des éléments (en octets)

La mise en place d'une taille maximale pour les éléments (en octets) permet de lutter contre les attaques par débordement de tampon (buffer overflow).

URL (domaine + chemin)	Taille maximum d'une URL, nom de domaine et chemin compris [128 – 4096 octets]
Par paramètre (après le « ? »)	Taille maximum d'un paramètre dans une URL [128 – 4096 (octets)]
Requête complète (URL+paramètres)	Nombre maximal d'octets pour la requête entière : http://URLBuffer ?QueryBuffer [128 – 4096] (octets)]

En-têtes HTTP : taille maximale des éléments (en octets)

Nombre de lignes par requête cliente	Nombre maximum de lignes (ou headers) que peut contenir une requête, du client vers le serveur (Min :16 ; Max : 512).
Nombre de lignes par réponse serveur	Nombre maximum de lignes (ou headers) que peut contenir une réponse du serveur vers le client (Min :16 ; Max : 512).
Champ AUTHORIZATION	Nombre maximum d'octets pour le champ AUTHORIZATION incluant les attributs de formatage. (Min : 128 ; Max : 4096).
Champ CONTENTTYPE	Nombre maximum d'octets pour le champ CONTENTTYPE incluant les attributs de formatage. (Min : 128 ; Max : 4096).
Champ HOST	Nombre maximum d'octets pour le champ HOST incluant les attributs de formatage. (Min : 128 ; Max : 4096).
Champ COOKIE	Nombre maximum d'octets pour le champ COOKIE incluant les attributs de formatage. (Min : 128 ; Max : 4096).

Analyses HTML/JavaScript

Inspecter le code HTML	Plutôt que d'interdire la connexion TCP, l'analyse efface les attributs malveillants pouvant être contenus dans le code HTML, en laissant passer le reste de la réponse.
Inspecter le code JavaScript	Afin d'éviter que des contenus malveillants ne viennent endommager les pages web dynamiques et interactives que fournit le langage de programmation JavaScript, une analyse est effectuée afin de les détecter. De la même façon que l'option **Inspecter le code HTML**, si cette case est cochée, l'analyse sera effectuée en effaçant les contenus malveillants, sans bloquer le paquet.
Supprimer automatiquement les contenus malveillants	Si cette case est cochée, tout code malicieux pouvant s'introduire dans du code HTML ou JavaScript sera automatiquement supprimé. **Exemple d'action malveillante :** Toute redirection à votre insu, vers un site web non souhaité.

Liste d'exclusion de la suppression automatique de code malveillant (User-Agent)

Celle-ci regroupe les navigateurs et leurs données qui ne seront pas supprimés automatiquement par l'option cité ci-dessus. Il est possible d'**Ajouter** ou de **Supprimer** des éléments de cette liste en cliquant sur les boutons du même nom.

Paramètres de sessions HTTP (en secondes)

Durée max. d'une requête	Programmée à 30 secondes par défaut (Max : 600 secondes).

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'action « passer » sera automatiquement déclenchée au sein du filtrage URL.
Tracer chaque requête HTTP	Active ou désactive les logs permettant de tracer les requêtes HTTP.

Onglet « Proxy »

Connexion

Conserver l'adresse IP source originale	Lorsqu'une requête est effectuée par un client web (navigateur) vers le serveur, le firewall l'intercepte et vérifie que celle-ci soit conforme aux règles de filtrage d'URL puis il relaie la demande. Si cette option est cochée, cette nouvelle requête utilisera l'adresse IP source originale du client web qui a émis le paquet. Dans le cas contraire, c'est l'adresse du firewall qui sera utilisée.

Extensions du protocole HTTP

Autoriser les connexions WebDAV (lecture et écriture)	WebDAV est un ensemble d'extensions au protocole HTTP concernant l'édition et la gestion collaborative de documents. Si cette option est cochée, le protocole WebDav est autorisé au travers du firewall NETASQ.
Autoriser les tunnels TCP (méthode CONNECT)	La **méthode CONNECT** permet de réaliser des tunnels sécurisés au travers de serveurs proxies. Si cette option est cochée la méthode **CONNECT** est autorisée au travers du firewall NETASQ.

Tunnels TCP : Liste des ports de destinations autorisés

Cette zone sert à spécifier quels types de service peuvent utiliser la méthode **CONNECT**.

Port de destination (objet service)	Le bouton **Ajouter** vous permet d'ajouter des services via la base d'objets. Pour **modifier** un service, sélectionnez la ligne à modifier puis faites votre nouvelle sélection. Le bouton **Supprimer** vous permet de supprimer le service sélectionné.

Configuration avancée

Proxy explicite

Le proxy explicite permet de référencer le proxy dans un navigateur et de lui transmettre directement les requêtes HTTP.

Autoriser plusieurs utilisateurs par adresse IP	Cette option permet d'attribuer une adresse IP commune à plusieurs utilisateurs

Qualité de la protection

Vérifier l'encodage de l'URL	En cochant cette option, la politique de filtrage ne peut être contournée.

Trafic émis vers le serveur

Ajouter l'utilisateur authentifié dans l'en-tête HTTP	Si le proxy HTTP externe nécessite une authentification des utilisateurs, l'administrateur peut cocher cette option pour envoyer au proxy externe les informations concernant l'utilisateur recueilli par le module d'authentification du firewall.

Onglet « ICAP »

Les contenus Web et Mail sont principalement visés par le protocole ICAP. Il fournit une interface aux proxies HTTP (pour le web) et aux relais SMTP (pour les mails).

Requête HTTP (reqmod)

Transmettre les requêtes HTTP au serveur ICAP	Chaque requête cliente vers un site web est transmise au serveur ICAP.

Serveur ICAP

Serveur	Indication du serveur ICAP.
Port Icap	Indication du port ICAP.
Nom du service ICAP	Indication du nom du service à mettre en place. Cette information est différente suivant la solution utilisée, le serveur ICAP ainsi que le port utilisé.

Authentification sur le serveur ICAP

On peut utiliser les informations disponibles sur le firewall pour réaliser des services ICAP.

Exemple

Il est possible de définir dans un serveur ICAP que tel ou tel site n'est destiné qu'à telle ou telle personne. Dans ce cas, vous pouvez filtrer selon un identifiant LDAP ou une adresse IP.

Transmettre le nom d'utilisateur/le groupe	Cette option permet de se servir des informations relatives à la base LDAP (notamment l'identifiant d'un utilisateur authentifié).
Transmettre l'adresse IP du client	Cette option permet de se servir des adresses IP des clients HTTP effectuant la requête à Adapter (objet utilisé pour faire la traduction entre le format ICAP et le format demandé).

Réponse HTTP (respmod)

Transmettre les réponses HTTP au serveur ICAP	Chaque réponse du serveur HTTP vers le client est transmise au serveur ICAP.

Serveur ICAP

Serveur	Indication de la machine ICAP.
Port	Indication du port ICAP.
Nom du service Icap	Indication du nom du service à mettre en place. Cette information est différente suivant la solution utilisée, le serveur ICAP ainsi que le port utilisé.

Authentification sur le serveur ICAP

On peut utiliser les informations disponibles sur le firewall pour réaliser des services ICAP.
Exemple
Il est possible de définir dans un serveur ICAP que tel ou tel site n'est destiné qu'à telle ou telle personne. Dans ce cas, vous pouvez filtrer selon un identifiant LDAP ou une adresse IP.

Transmettre le nom d'utilisateur/le groupe	Cette option permet de se servir des informations relatives à la base LDAP (notamment l'identifiant d'un utilisateur authentifié).
Transmettre l'adresse IP du client P	Cette option permet de se servir des adresses IP des clients HTTP effectuant la requête à Adapter.

Configuration avancée

Liste blanche (pas de transmission au serveur ICAP)

Serveur HTTP (Machine – Réseau – Plage d'adresse)	Permet d'ajouter des machines, des réseaux ou des plages d'adresses dont les informations ne seront pas transmises au serveur ICAP. Ceux-ci peuvent être supprimés de la liste à tout moment.

Onglet « Analyse des fichiers »

Transfert de fichiers

Téléchargement partiel	Par exemple lorsqu'on télécharge un fichier via HTTP si le téléchargement ne s'effectue pas jusqu'au bout (erreur de connexion par exemple), il est possible de relancer le téléchargement à partir de là où a surgi l'erreur plutôt que de devoir tout télécharger de nouveau. Il s'agit dans ce cas d'un téléchargement partiel (le téléchargement ne correspond pas à un fichier complet). L'option **Téléchargement partiel** permet de définir le comportement du proxy HTTP du firewall vis-à-vis de ce type de téléchargement. • **Bloquer** : le téléchargement partiel est interdit • **Bloquer si l'antivirus est actif** : le téléchargement partiel est autorisé et le trafic est filtré par l'antivirus. • **Passer** : le téléchargement partiel est autorisé mais il n'y a pas d'analyse antivirale effectuée.
Taille maximale d'un fichier [0-2147483647(Ko)]	Lorsque les fichiers téléchargés sur l'Internet, via HTTP, sont trop imposants, ils peuvent dégrader la bande passante du lien Internet et cela pour une durée parfois très longue. Pour éviter cela, indiquez la taille maximum en Ko pouvant être téléchargée par le protocole HTTP.

Filtrage des fichiers (par type MIME)

Etat	Indique l'état actif ou inactif du fichier. 2 positions sont disponibles : « Activé » ou « Désactivé »
Action	Indique l'action à mettre en place pour le fichier en question, il existe 3 possibilités : • **Détecter et bloquer les virus** : Le fichier est analysé afin de détecter les virus pouvant s'y être glissé, ceux-ci seront bloqués. • **Passer sans analyse antivirale** : Le fichier peut être téléchargé librement, aucune analyse antivirale n'est effectuée. • **Bloquer** : Le téléchargement du fichier est interdit.
Type MIME	Indique de quel type de contenu de fichier il s'agit. Cela peut être du texte, de l'image ou de la vidéo, à définir dans ce champ. **Exemples** : « text/plain* » « text/* » « application/* »
Taille max. pour l'analyse antivirale (Ko)	Ce champ correspond à la taille maximale qu'un fichier peut atteindre afin qu'il soit analysé. Celle-ci est fixée à 1000 Ko par défaut.

Actions sur les fichiers

Lorsqu'un virus est détecté	Ce champ contient 2 options. En sélectionnant « Bloquer », le fichier analysé n'est pas transmis. En sélectionnant « Passer », l'antivirus transmet le fichier dans son état.
Lorsque l'antivirus ne peut analyser	Cette option définit le comportement de l'antivirus si l'analyse du fichier qu'il est en train de scanner échoue. **Exemple :** Il ne réussit pas à analyser le fichier parce qu'il est verrouillé. Si **Bloquer** est spécifié, le fichier en cours d'analyse n'est pas transmis.

	Si **Passer sans analyser** est spécifié, le fichier en cours d'analyse est transmis.
Lorsque la collecte de données échoue	Cette option décrit le comportement de l'antivirus face à certains événements. Il est possible de **Bloquer** le trafic en cas d'échec de la récupération des informations, ou de le laisser **passer sans analyser**. **Exemple :** Si le disque dur est plein, le téléchargement des informations ne pourra pas être effectué.

SMTP

Le protocole SMTP a pour objectif de détecter les connexions entre un client et un serveur e-mail ou entre deux serveurs e-mails utilisant le protocole SMTP. Il permet d'envoyer des e-mails. Il est utilisé par SEISMO pour détecter la version du client et/ou du serveur e-mail afin de remonter d'éventuelles vulnérabilités.

Onglet « IPS »

Détecter et inspecter automatiquement le protocole	Si le protocole est activé, il est automatiquement utilisé à la découverte d'un paquet correspondant dans les règles de filtrage. Cette option n'est pas disponible pour les protocoles IP, ICMP TCPUDP, RTP, RTCP, MSN, YMSG.

Extensions du protocole SMTP

Filtrer l'extension CHUNKING	Permet de filtrer les données transférées d'une adresse mail à une autre. **Exemple :** Les pièces jointes incluses dans un mail.
Filtrer les extensions spécifiques à Microsoft Exchange Server	Permet de filtrer les commandes additionnelles provenant du serveur de mails Microsoft Exchange Server.
Filtrer la demande de notification de sens de connexion ATRN et ETRN	Permet de filtrer les données contenues dans la demande de notification de sens de connexion, du client vers le serveur, ou du serveur vers le client. Lors d'une communication SMTP, l'utilisation des commandes ATRN et ETRN permet d'échanger les rôles client/serveur.

Taille maximale des éléments (Ko)

La mise en place d'une taille maximale pour les éléments (en Ko) permet de lutter contre les attaques par débordement de tampon (buffer overflow).

En-tête du message **[64 – 4096]**	Nombre maximum de caractères que peut contenir l'en-tête d'un e-mail (adresse mail de l'expéditeur, date, type de codage utilisé etc.)
Ligne de réponse serveur [64 – 4096]	Nombre maximum de caractères que peut contenir la ligne de réponse du serveur SMTP.
Données Exchange (XEXCH50) **[102400 – 1073741824]**	Taille maximale des données lors d'un transfert de fichier au format MBDEF (Message Database Encoding Format).
En-tête de l'extension BDAT	Taille maximale des données transmises via la commande BDAT.

[102400 – 10485760]	
Ligne de commande **[64 – 4096]**	Taille maximale des données que peut contenir une ligne de commande (en dehors de la commande DATA).

Support

Désactiver la prévention d'intrusion	En cochant cette option, la configuration venant d'être effectuée au travers des différents champs compris dans l'onglet ne sera pas prise en compte.
Tracer chaque requête SMTP	Active ou désactive les logs permettant de tracer les requêtes SMTP.

Onglet « Proxy »

Filtrer la bannière d'accueil	Lorsque cette option est cochée, la bannière du serveur est anonymisée lors d'une connexion SMTP.

Commande HELO

Remplacer le nom de domaine du client par son adresse IP	Lors d'une identification basique, le client renseigne son nom de domaine en exécutant la commande HELO. En cochant cette case, le nom de domaine sera remplacé par l'adresse IP.

Connexion

Conserver l'adresse IP source originale	Lorsqu'une requête est effectuée par un client web (navigateur) vers le serveur, le firewall l'intercepte et vérifie que celle-ci soit conforme aux règles de filtrage d'URL puis il relaie la demande. Si cette option est cochée, cette nouvelle requête utilisera l'adresse IP source originale du client web qui a émis le paquet. Dans le cas contraire, c'est l'adresse du firewall qui sera utilisée.

Limites lors de l'envoi d'un e-mail

Ligne de message **[1000-2048 (Ko)]**	Ce champ indique la longueur maximale d'une ligne lors de l'envoi d'un message. **REMARQUE** La mise en place d'une taille maximale pour les éléments (en octets) permet de lutter contre les attaques par débordement de tampon (buffer overflow).
Nombre maximal de destinataires **[0 – 2147483647 (Ko)]**	Indique le nombre maximum de destinataires que peut contenir un message. Les messages dont le nombre de destinataires est excessif seront refusés par le firewall (le refus sera marqué par un message d'erreur SMTP). Cela permet de limiter le spam d'e-mails.
Taille maximum du message **[0 – 2147483647 (Ko)]**	Indique la taille maximale que peut prendre un message passant par le firewall NETASQ. Les messages dont la taille est excessive seront refusés par le firewall.

Onglet « Commandes SMTP»

Ce menu vous permet d'autoriser ou de rejeter les commandes SMTP définies dans les RFC. Vous pouvez laisser passer une commande, la bloquer ou analyser la syntaxe et vérifier que la commande est conforme aux RFC en vigueur.

Proxy

<u>Commandes principales</u>

Bouton **Modifier toutes les commandes** : Permet d'autoriser, de rejeter ou de vérifier toutes les commandes.

Commande	Indication du nom de la commande.
Action	Indication de l'action effectuée.

<u>Autres commandes autorisées</u>

Commande	Par défaut, toutes les commandes non définies dans les RFC sont interdites. Cependant, certains systèmes de messagerie utilisent des commandes supplémentaires non standardisées. Vous pouvez donc ajouter ces commandes afin de les laisser passer au travers du firewall. Les boutons d'actions **Ajouter** et **Supprimer** permettent d'agir sur la liste de commandes.

IPS

<u>Commandes SMTP autorisées</u>

Liste des commandes SMTP supplémentaires autorisées. Il est possible d'en **Ajouter** ou d'en **Supprimer**.

<u>Commandes SMTP interdites</u>

Liste des commandes SMTP interdites. Il est possible d'en **Ajouter** ou d'en **Supprimer**.

Onglet « Analyse des fichiers»

Taille max. pour l'analyse antivirale [0 – 1000 (Ko)]	Cette option est fonction des capacités matérielles de chaque modèle de firewall mais elle peut être adaptée selon les besoins de l'entreprise.



AVERTISSEMENT

Lorsque vous définissez une taille limite de données analysées manuellement, veillez à conserver un ensemble de valeurs cohérentes. En effet, l'espace mémoire total correspond à l'ensemble des ressources réservées pour le service Antivirus. Si vous définissez que la taille limite des données analysées sur SMTP est de 100% de la taille totale, aucun autre fichier ne pourra être analysé en même temps.

Action sur les messages

Cette zone décrit le comportement de l'antivirus face à certains événements.

Lorsqu'un virus est détecté	Ce champ contient 2 options : « Passer » et « Bloquer ». En sélectionnant « Bloquer », le fichier analysé n'est pas transmis. En sélectionnant « Passer », l'antivirus transmet le fichier même s'il est détecté comme infecté.
Lorsque l'antivirus ne peut analyser	L'option **Passer sans analyser** définit le comportement de l'antivirus si l'analyse du fichier qu'il est en train de scanner échoue Si **Bloquer** est spécifié, le fichier en cours d'analyse n'est pas transmis. Si **Passer sans analyser** est spécifié, le fichier en cours d'analyse est transmis.

Lorsque la collecte de données échoue	Cette option décrit le comportement de l'antivirus face à certains événements. **Exemples :** Si le disque dur est plein, le téléchargement des informations ne pourra pas être effectué. La taille maximale que le fichier peut atteindre pour l'analyse antivirale est restreinte (1000Ko).

POP3

Le protocole POP3 a pour objectif de détecter les connexions entre un client et un serveur e-mail utilisant le protocole POP3.

Onglet « IPS - PROXY »

Ces deux fonctionnalités ont été réunies en un seul onglet par souci d'ergonomie.

IPS

Détecter et inspecter automatiquement le protocole	Si le protocole est activé, il est automatiquement utilisé à la découverte d'un paquet correspondant dans les règles de filtrage. Cette option n'est pas disponible pour les protocoles, IP, ICMP TCPUDP, RTP, RTCP, MSN, YMSG.

Proxy

Le trafic Mail n'est pas seulement basé sur le protocole SMTP mais aussi sur POP3. Ce protocole va permettre à l'utilisateur d'un logiciel de messagerie, de récupérer sur son poste des mails stockés sur un serveur distant. Ce serveur de mail distant pouvant être situé à l'extérieur du réseau local ou sur une interface distincte, le flux POP3 transite au travers du firewall lui permettant de réaliser son analyse.

Filtrer la bannière d'accueil envoyée par le serveur	Lorsque cette option est cochée, la bannière de votre serveur de messagerie n'est plus envoyée lors d'une connexion POP3. En effet, cette bannière contient des informations qui peuvent être exploitées par certains pirates (type de serveur, version logicielle ...).

Connexion

Conserver l'adresse IP source originale	Lorsqu'une requête est effectuée par un client web (navigateur) vers le serveur, le firewall l'intercepte et vérifie que celle-ci soit conforme aux règles de filtrage d'URL puis il relaie la demande. Si cette option est cochée, cette nouvelle requête utilisera l'adresse IP source originale du client web qui a émis le paquet. Dans le cas contraire, c'est l'adresse du firewall qui sera utilisée.

Support

Désactiver la prévention d'intrusion	En cochant cette option, la configuration venant d'être effectuée au travers des différents champs ne sera pas prise en compte.
Tracer chaque requête POP3	Active ou désactive les logs permettant de tracer les requêtes HTTP.

Onglet « Commandes POP3»

Proxy

Commandes principales

Ce menu vous permet d'autoriser ou de rejeter les commandes POP3 définies dans les RFC. Vous pouvez laisser passer une commande, la bloquer ou analyser la syntaxe et vérifier que la commande est conforme aux RFC en vigueur.
Bouton **Modifier toutes les commandes :** Permet d'autoriser, de rejeter ou de vérifier toutes les commandes.

Commande	Indication du nom de la commande
Action	Cela permet de définir le comportement attribué à la commande.3 possibilités sont disponibles. Il faut cliquer sur l'action de la commande pour pouvoir la modifier : • **Analyser** : les données liées à la commande sont analysées en conformité avec les RFC, et bloquées si nécessaire. **Exemple :** Si le nom de la commande USER n'est pas conforme aux RFC, le paquet ne sera pas transmis au serveur. • **Passer sans analyser** : la commande est autorisée, sans vérification. • **Bloquer** : la commande est bloquée d'office, une alarme sera remontée pour le stipuler.

Autres commandes autorisées

Commande	Ce champ permet d'ajouter des commandes personnelles supplémentaires.

Onglet « Analyse des fichiers»

Taille maximum pour l'analyse antivirale (Ko)	Cette option est fonction des capacités matérielles de chaque modèle de firewall. Elle correspond à la taille maximale qu'un fichier peut atteindre afin qu'il soit analysé. Celle-ci est fixée à 1000 Ko.



Lorsque vous définissez une taille limite de données analysées manuellement, veillez à conserver un ensemble de valeurs cohérentes. En effet, l'espace mémoire total correspond à l'ensemble des ressources réservées pour le service Antivirus. Si vous définissez que la taille limite des données analysées sur POP3 est de 100% de la taille total, aucun autre fichier ne pourra être analysé en même temps.

Action sur les messages

Cette zone décrit le comportement de l'antivirus face à certains événements.

Lorsqu'un virus est détecté	Ce champ contient 2 options. En sélectionnant « Bloquer », le fichier analysé n'est pas transmis. En sélectionnant « Passer », l'antivirus transmet le fichier dans son état.
Lorsque l'antivirus ne peut analyser	Cette option définit le comportement de l'antivirus si l'analyse du fichier qu'il est en train de scanner échoue. **Exemple** Il ne réussit pas à analyser le fichier parce qu'il est verrouillé. Si **Bloquer** est spécifié, le fichier en cours d'analyse n'est pas transmis. Si **Passer sans analyser** est spécifié, le fichier est transmis sans vérification.
Lorsque la collecte de données échoue	Cette option décrit le comportement de l'antivirus face à certains événements. Il est possible de **Bloquer** le trafic en cas d'échec de la récupération des informations, ou de le laisser **passer sans analyser**.

FTP

Onglet « IPS »

Le protocole FTP supporte la RFC principale [RFC959] ainsi que de nombreuses extensions. L'activation de ce protocole permet de prévenir des grandes familles d'attaques applicatives basées sur le protocole FTP. Ce protocole effectue diverses analyses comme l'analyse de conformité aux RFC, la vérification de la taille des paramètres des commandes FTP ou les restrictions sur le protocole (SITE EXEC par exemple). Ces analyses, permettent ainsi de stopper les attaques comme FTP Bounce, FTP PASV DoS, Buffer Overflow…Ce protocole est indispensable pour permettre au trafic FTP de traverser le firewall et de gérer dynamiquement les connexions de données du protocole FTP.

Détecter et inspecter automatiquement le protocole	Si le protocole est activé, il est automatiquement utilisé à la découverte d'un paquet. Cette option n'est pas disponible pour les protocoles IP, ICMP TCPUDP, RTP, RTCP, MSN, YMSG.

Authentification

Autoriser l'authentification SSL	Activation du support de l'authentification SSL pour le protocole (FTP uniquement). En cochant cette option, les données personnelles comme le login et le mot de passe pourront être chiffrées, et donc, protégées.
Ne pas analyser la phase d'authentification FTP	Aucune vérification des données ne sera effectuée

Taille des éléments (en octets)

La mise en place d'une taille maximale pour les éléments (en octets) permet de lutter contre les attaques par débordement de tampon (buffer overflow).

Nom d'utilisateur	Nombre maximum de caractères que peut contenir un nom d'utilisateur : Celui-ci est compris entre 10 et 2048 octets.
Mot de passe utilisateur	Nombre maximum de caractères pour le mot de passe FTP. Il doit être compris entre 10 et 2048 octets.
Chemin (répertoire + nom de fichier)	Nombre maximum de caractères que peut contenir le parcours suivi par l'exécution du programme, soit le circuit emprunté dans l'arborescence pour parvenir au fichier FTP. Ce nombre est compris entre 10 et 2048 octets.
Commande SITE	Nombre maximum de caractères que peut contenir la commande SITE (entre 10 et 2048 octets).
Autres commandes	Nombre maximum de caractères que peut contenir les commandes supplémentaires (entre 10 et 2048 octets)

Support

Désactiver la prévention d'intrusion	En cochant cette option, le profil venant d'être configuré ne sera pas pris en compte.
Tracer chaque requête FTP	Activation ou désactivation de la remontée des logs concernant le protocole FTP.

Onglet « Proxy »

Filtrer la bannière d'accueil envoyée par le serveur FTP	En cochant cette option, la bannière du serveur ne sera plus envoyée lors d'une connexion FTP.
Interdire les rebonds (FTP bounce)	Permet d'éviter le spoofing, ou usurpation d'adresse IP. Une machine extérieure, en exécutant la commande PORT et en spécifiant une adresse IP interne, pourrait accéder à des données confidentielles, en exploitant les failles d'un serveur FTP ou d'une machine vulnérables par « rebond ».

Connexion

Conserver l'adresse IP source originale	Lorsqu'une requête est effectuée par un client web (navigateur) vers le serveur, le firewall l'intercepte et vérifie que celle-ci soit conforme aux règles de filtrage d'URL puis il relaie la demande. Si cette option est cochée, cette nouvelle requête utilisera l'adresse IP source originale du client web qui a émis le paquet. Dans le cas contraire, c'est l'adresse du firewall qui sera utilisée.

Modes de transfert autorisés

Entre le client et le proxy	Lorsque le client FTP envoie une requête au serveur, celle-ci est d'abord interceptée par le proxy qui l'analyse. Du point de vue du « client » FTP, le proxy correspond au serveur. Cette option permet de définir le mode de transfert autorisé : Si **Actif uniquement** est spécifié, le client FTP détermine le port de connexion à utiliser pour transférer les données. Le serveur FTP initialisera la connexion de son port de données (port 20) vers le port spécifié par le client. Si **Passif uniquement** est spécifié, le serveur FTP détermine lui-même le port de connexion à utiliser afin de transférer les données (data connexion) et le transmet au client. Si **Actif et passif** est spécifié, le client FTP aura le choix entre les deux modes de transfert au moment de la configuration du firewall.
Entre le proxy et le serveur	Lorsque le proxy a terminé l'analyse de la requête cliente, il la transfère au serveur FTP. Ce dernier interprète le proxy comme le client FTP, puisque le proxy a un rôle intermédiaire, il est transparent. Les modes de transfert autorisés sont les mêmes que pour l'option précédente.

Onglet « Commandes »

Proxy

Commandes principales

Bouton **Modifier les commandes d'écriture :** Ce bouton permet de passer sans analyser bloquer ou analyser la syntaxe et vérifier que la commande est conforme aux RFC en vigueur, ceci, pour les commandes d'écriture.
Bouton **Modifier toutes les commandes :** Ce bouton permet de passer sans analyser, bloquer ou analyser la syntaxe et vérifier que la commande est conforme aux RFC en vigueur, ceci, aussi bien pour les commandes génériques que les commandes de modification.

Commande	Nom de la commande.
Action	3 autorisations possibles entre « Passer sans analyser », « Analyser » et « Bloquer ».
Type de commande	Indication du type de commande. Les commandes FTP dites «d'écriture» définies dans les RFC sont des commandes pouvant entraîner des modifications au niveau du serveur comme, par exemple, la suppression de données ou encore la création de répertoires. Le fonctionnement de ces commandes est identique aux commandes dites « génériques » : en effet, vous pouvez laisser passer une commande, la bloquer ou analyser la syntaxe et vérifier que la commande est conforme aux RFC en vigueur.

Autres commandes autorisées

Il est possible d'**Ajouter** des commandes supplémentaires, dans la limite de 21 caractères, et de les **Supprimer** si besoin.

IPS

Commandes FTP autorisées

Il est possible de définir des commandes FTP au sein de la prévention d'intrusion, en cliquant sur **Ajouter**, dans la limite de 115 caractères. La suppression est également autorisée.

Commandes FTP interdites

Il est possible d'interdire des commandes FTP au sein de la prévention d'intrusion, dans la limite de 115 caractères.

Onglet « Analyse des fichiers »

Taille maximum pour l'analyse antivirale [0 – 1000] (Ko)	Il est possible ici de déterminer la taille maximale utilisée pour l'analyse des fichiers. Pour cela, déplacez la réglette. Vous pouvez également configurer l'action à entreprendre si le fichier est supérieur à la taille autorisée. **AVERTISSEMENT** Lorsque vous définissez une taille limite de données analysées manuellement, veillez à conserver un ensemble de valeurs cohérentes. En effet, l'espace mémoire total, représenté par la réglette correspond à l'ensemble des ressources réservées pour le service Antivirus. Si vous définissez que la taille limite des données analysées sur SMTP est de 100% de la taille total, aucun autre fichier ne pourra être analysé en même temps.
Analyser les fichiers	Cette option permet de choisir le type de fichier devant être analysé : les fichiers « téléchargés et envoyés » ; les fichiers « téléchargés uniquement » ou les fichiers « envoyés uniquement ».

Actions sur les fichiers

Lorsqu'un virus est détecté	Cette option propose deux actions : « Passer » et « Bloquer ». En sélectionnant « Bloqué », le fichier analysé n'est pas transmis. En sélectionnant « Passer », l'antivirus transmet le fichier en cours d'analyse.
Lorsque l'antivirus ne peut analyser	Cette option définit l'état de l'antivirus si l'analyse du fichier qu'il est en train de scanner échoue Exemple Il ne réussit pas à analyser le fichier parce qu'il est verrouillé. Si Bloquer est spécifié, le fichier en cours d'analyse n'est pas transmis. Si Passer sans analyser est spécifié, le fichier en cours d'analyse est transmis.
Lorsque la collecte des données échoue	Cette option décrit le comportement de l'antivirus face à certains événements. Il est possible de **Bloquer** le trafic en cas d'échec de la récupération des informations, ou de le laisser **passer sans analyser**

SSL

Onglet « IPS »

Cet écran va permettre valider le fonctionnement du protocole SSL à travers le firewall.
Certaines options permettent de renforcer la sécurité de ce protocole. Par exemple, il est possible d'interdire des négociations d'algorithmes cryptographiques considérés comme faibles, de détecter des logiciels utilisant le SSL pour passer outre les politiques de filtrage (SKYPE, proxy HTTPS,…).

Détecter et inspecter automatiquement le protocole	Si le protocole est activé, il est automatiquement utilisé à la découverte d'un paquet correspondant dans les règles de filtrage. Cette option n'est pas disponible pour les protocoles IP, ICMP TCPUDP, RTP, RTCP, MSN, YMSG.

Négociation SSL

Autoriser les chiffrements non supportés	Cochez cette case si l'algorithme de chiffrement que vous souhaitez utiliser n'est pas supporté par le protocole SSL.
Autoriser les données non chiffrées	Cette option permet de transmettre les données en clair après une négociation SSL. **AVERTISSEMENT** Laisser transiter les données en clair représente un risque de sécurité.
Niveaux de chiffrements autorisés	Plus l'algorithme de chiffrement utilisé est fort, et le mot de passe complexe, plus le niveau est considéré comme « haut ». **Exemple** L'algorithme de chiffrement AES doté d'une force de 256 bits, associé à un mot de passe d'une dizaine de caractères fait de lettres, de chiffres et de caractères spéciaux. Trois choix sont proposés, vous pouvez autoriser les niveaux de chiffrement :

	Bas, moyen et haut : par exemple, DES (force de 64 bits), CAST128 (128 bits) et AES. Quelque soit le niveau de sécurité du mot de passe, le niveau de chiffrement sera autorisé. **Moyen et haut** : Seuls les algorithmes de moyenne et haute sécurité seront tolérées. **Haut uniquement** : Seuls les algorithmes forts et les mots de passe dotés d'un haut niveau de sécurité seront tolérés.

Détection des données non chiffrées (trafic en clair)

Méthode de détection	**Ne pas détecter** : les données non chiffrées ne seront pas analysées. **Inspecter tout le flux** : tous les paquets reçus seront analysés par le protocole SSL afin de détecter du trafic en clair **Echantillonage (7168 octets)** : Seuls les 7168 premiers octets du flux seront analysés afin de détecter du trafic en clair.

Résolution des problèmes

Désactiver l'IPS	En cochant cette option, la configuration venant d'être effectuée au travers des différents champs compris dans l'onglet ne sera pas prise en compte
Activer les traces	Active ou désactive les logs permettant de tracer les requêtes SMTP.
Désactiver la détection de Skype	L'application Skype utilise le port 443 et un protocole ressemblant à du SSL valide. Toutefois, plusieurs concurrents bloquent l'utilisation du Skype. Cette option permet de débloquer le trafic SKYPE sans pour autant arrêter d'analyser le SSL. Il suffit de cocher cette option pour bloquer le trafic SKYPE.

Onglet « Proxy »

Connexion

Conserver l'adresse IP source originale	Lorsqu'une requête est effectuée par un client web (navigateur) vers le serveur, le firewall l'intercepte et vérifie que celle-ci soit conforme aux règles de filtrage d'URL puis il relaie la demande. Si cette option est cochée, cette nouvelle requête utilisera l'adresse IP source originale du client web qui a émis le paquet. Dans le cas contraire, c'est l'adresse du firewall qui sera utilisée.

Inspection de contenu

Certificats auto-signés	Cette option va déterminer l'action à effectuer lorsque vous rencontrez des certificats auto-signés : vous pouvez choisir de les **Bloquer** ou de **Continuer l'analyse** en les acceptant. Ces certificats sont à usage interne et signés par votre serveur local. Ils

	permettent de garantir la sécurité de vos échanges, et, entre autres, d'authentifier les utilisateurs.
Certificats expirés	Cette option va déterminer l'action à effectuer lorsque vous rencontrez des certificats auto-signés : vous pouvez choisir de les **Bloquer** ou de **Continuer l'analyse** en ne les considérant pas. Les certificats expirés sont antérieurs ou postérieurs à la date en cours et ne sont donc pas « valides ». Pour y remédier, ils doivent être renouveler par une autorité de certification. **AVERTISSEMENT** Les certificats expirés peuvent présenter un risque de sécurité. Après expiration d'un certificat, la CA l'ayant émis n'est plus responsable d'une utilisation malveillante de celui-ci.
Certificats inconnus	Cette option va déterminer l'action à effectuer lorsque vous rencontrez des certificats auto-signés : vous pouvez choisir de les **Bloquer** ou de **Continuer l'analyse** en ne les considérant pas.

Support

Si le déchiffrement échoue	Cette option va déterminer l'action à effectuer lorsque le déchiffrement échoue: vous pouvez choisir de **Bloquer le trafic** ou de **Passer sans déchiffrer**. En choisissant cette deuxième possibilité, le trafic ne sera pas inspecté.

TCP-UDP

Le protocole TCP assure le contrôle des données lors de leur transfert. Il a pour rôle de vérifier que les paquets IP envoyés sont bien reçus en l'état, sans aucune perte ou changement sur le plan de leur intégrité.
Le protocole UDP peut remplacer le TCP en cas de problème mineur, il assure un transfert plus fluide car il ne contrôle pas chacune des étapes de la transmission. Il convient par exemple à des applications de streaming (diffusion audio/vidéo) pour lesquelles la perte de paquets n'est pas vitale. En effet, lors de ces transmissions, les paquets perdus seront ignorés.

En choisissant TCP-UDP au sein de la liste, vous pouvez accéder à deux écrans :

- La configuration globale
- L'accès aux profils

L'écran des profils

Onglet « IPS-Connexion »

Inspection

Imposer une limite MSS	Cette case permet d'imposer une limite MSS (*Maximum Segment Size*) pour l'inspection du profil.  **NOTE**

	Le MSS désigne la quantité de données en octets qu'un ordinateur ou tout équipement de communication peut contenir dans un paquet seul et non fragmenté. En cochant cette option, vous dégriserez le champ suivant qui vous permettra d'établir votre limite.
Limite MSS (en octets)	Définissez votre limite MSS, comprise entre 100 et 65535 octets.
Réécrire les séquences TCP avec un aléa fort (arc4)	En cochant cette case, les numéros de séquence TCP générées par le client et le serveur seront écrasés et remplacés par le moteur de prévention d'intrusion NETASQ, qui produira des numéros de séquence aléatoires.
Protéger contre l'envoi répété de paquets ACK	En cochant cette option, vous vous protégez contre le vol de session, ou attaque de type « ACK ».

Expiration (en secondes)

Délai d'ouverture d'une connexion (SYN)	Définissez un délai d'ouverture pour une connexion, compris entre 10 et 60 secondes.
Connexion TCP	Définissez une durée de vie pour votre connexion TCP, comprise entre 30 et 604800 secondes.
Pseudo-connexion UDP	Définissez une durée de vie pour votre connexion UDP, comprise entre 30 et 3600 secondes.
Fermeture d'une connexion (FIN)	Définissez au bout de combien de temps la connexion doit être fermée, entre 10 et 3600 secondes.
Connexion fermée	Définissez en combien de temps la connexion doit être fermée, compris entre 10 et 60 secondes.
Petite fenêtre TCP	Définissez la durée de vie d'une petite fenêtre TCP, comprise entre 5 et 604800 secondes.

Support

Désactiver le proxy SYN	En cochant cette case, vous ne serez plus protégé contre les attaques de type « SYN », car le proxy ne filtrera plus les paquets.

L'écran de la configuration globale

Onglet « IPS »

Déni de Service (DoS)

Nombre max. de ports par seconde	Ce nombre doit être compris entre 1 et 16 ports par seconde.
Fréquence de purge table de session (secondes)	Définissez au bout de combien de temps la purge des tables de sessions doit être effectuée, compris entre 10 et 172800 secondes.

Connexion

Autoriser les connexions semi-ouvertes (RFC 93, section 3.4)	Cette option permet d'éviter le déni de service pouvant opérer au sein des connexions dites « normales ».

IP

Onglet « IPS »

MTU

Imposer une limite MTU (force la fragmentation)	Le MTU (*Maximum Transmission Unit*) représente la taille maximale d'un paquet IP. En cochant cette option, vous dégriserez la suivante et pourrez définir votre limite.
Valeur maximale du MTU	Définissez la valeur maximale du datagramme IP, comprise entre 140 et 65535 octets.

Fragmentation

Taille minimum d'un fragment (octets)	Le fragment doit être compris entre 140 et 65535 octets.
Expiration d'une session (en secondes)	Cela doit être compris entre 2 et 30 secondes.



Le protocole IP ne dispose pas de profil.

ICMP

Onglet « IPS »

Paramètres de session (en secondes)

Expiration d'une session	Cette valeur doit être comprise entre 2 et 60 secondes.

Support

Ignorer les notifications ICMP (suivi d'état TCP/UDP)	En cochant cette option, vous ne prendrez pas en compte les messages d'erreur pouvant intervenir au sein des protocoles, comme l'inaccessibilité d'un service ou d'un hôte, par exemple.

DNS

L'écran des profils

Onglet « IPS »

Détecter et inspecter automatiquement le protocole	Si le protocole est activé, il est automatiquement utilisé à la découverte d'un paquet correspondant dans les règles de filtrage. Cette option n'est pas disponible pour les protocoles, IP, ICMP TCPUDP, RTP, RTCP, MSN, YMSG.

Taille maximale des champs DNS (en octets)

Nom DNS (requête)	Ce champ doit être compris entre 10 et 2048 octets.

Liste blanche de domaines DNS (DNS rebinding)

Cette liste contient les noms de domaines autorisés (de type <*www.dedomaine.fr*>, par exemple) à être résolus par un serveur se trouvant sur une interface non-protégée.
Vous pouvez en ajouter en cliquant sur le bouton approprié, ou le retirer de la liste en le sélectionnant et en cliquant sur « Supprimer ».

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'action « passer » sera automatiquement déclenchée au sein du filtrage URL.

L'écran de la configuration globale

DNS : liste des ports UDP par défaut

Cette liste contient les ports UDP autorisés par défaut.
Vous pouvez en ajouter en cliquant sur le bouton approprié, ou le retirer de la liste en le sélectionnant et en cliquant sur « Supprimer ».

Yahoo Messenger (YMSG)

L'écran des profils

Onglet « IPS »

Détecter et inspecter automatiquement le protocole	Si le protocole est activé, il est automatiquement utilisé à la découverte d'un paquet correspondant dans les règles de filtrage. Cette option n'est pas disponible pour les protocoles, IP, ICMP TCPUDP, RTP, RTCP, MSN, YMSG.

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'action « passer » sera automatiquement déclenchée au sein du filtrage URL.
Tracer chaque requête Yahoo Messenger	Active ou désactive la remontée des logs relatifs au protocole Yahoo Messenger.

L'écran de la configuration globale

YMSG : liste des ports TCP par défaut

Cette liste contient les ports TCP autorisés par défaut.
Vous pouvez en ajouter en cliquant sur le bouton approprié, ou le retirer de la liste en le sélectionnant et en cliquant sur « Supprimer ».

ICQ – AOL IM (OSCAR)

L'écran des profils

Onglet « IPS »

Détecter et inspecter automatiquement le protocole	Si le protocole est activé, il est automatiquement utilisé à la découverte d'un paquet correspondant dans les règles de filtrage. Cette option n'est pas disponible pour les protocoles, IP, ICMP TCPUDP, RTP, RTCP, MSN, YMSG.

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'action « passer » sera automatiquement déclenchée au sein du filtrage URL.
Tracer chaque requête OSCAR	Active ou désactive les logs permettant de tracer les requêtes OSCAR.

L'écran de la configuration globale

OSCAR : liste des ports TCP par défaut

Cette liste contient les ports TCP autorisés par défaut pour le protocole OSCAR.
Vous pouvez en ajouter en cliquant sur le bouton approprié, ou le retirer de la liste en le sélectionnant et en cliquant sur « Supprimer ».

OSCAR over SSL: liste des ports TCP par défaut

Cette liste contient les ports TCP autorisés par défaut pour le protocole OSCAR passant par le SSL.
Vous pouvez en ajouter en cliquant sur le bouton approprié, ou le retirer de la liste en le sélectionnant et en cliquant sur « Supprimer ».

Live Messenger (MSN)

L'écran des profils

Onglet « IPS »

Détecter et inspecter automatiquement le protocole	Si le protocole est activé, il est automatiquement utilisé à la découverte d'un paquet correspondant dans les règles de filtrage. Cette option n'est pas disponible pour les protocoles, IP, ICMP TCPUDP, RTP, RTCP, MSN, YMSG.

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'action « passer » sera automatiquement déclenchée au sein du filtrage URL.
Tracer chaque requête Live Messenger	Active ou désactive les logs permettant de tracer les requêtes Live Messenger.

L'écran de la configuration globale

MSN : liste des ports TCP par défaut

Cette liste contient les ports TCP autorisés par défaut pour MSN.
Vous pouvez en ajouter en cliquant sur le bouton approprié, ou le retirer de la liste en le sélectionnant et en cliquant sur « Supprimer ».

TFTP

L'écran des profils

Onglet « IPS »

Détecter et inspecter automatiquement le protocole	Si le protocole est activé, il est automatiquement utilisé à la découverte d'un paquet correspondant dans les règles de filtrage. Cette option n'est pas disponible pour les protocoles, IP, ICMP TCPUDP, RTP, RTCP, MSN, YMSG.

Taille des éléments (en octets)

Nom de fichier	Ce nombre doit être compris entre 64 et 512 octets.

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'action « passer » sera automatiquement déclenchée au sein du filtrage URL.
Tracer chaque requête TFTP	Active ou désactive permettant de tracer les requêtes TFTP.

L'écran de la configuration globale

TFTP : liste des ports UDP par défaut

Cette liste contient les ports TCP autorisés par défaut pour le protocole TFTP.
Vous pouvez en ajouter en cliquant sur le bouton approprié, ou le retirer de la liste en le sélectionnant et en cliquant sur « Supprimer ».

NetBios CIFS

NetBios est un protocole utilisé pour le partage de fichier/imprimantes, généralement par les systèmes Microsoft.

L'écran des profils

Onglet « IPS »

Détecter et inspecter automatiquement le protocole	Si le protocole est activé, il est automatiquement utilisé à la découverte d'un paquet correspondant dans les règles de filtrage. Cette option n'est pas disponible pour les protocoles, IP, ICMP TCPUDP, RTP, RTCP, MSN, YMSG.

Taille des éléments (en octets)

Nom des fichiers (format SMB2)	Ce nombre doit être compris entre 1 et 65536 octets.

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'action « passer » sera automatiquement déclenchée au sein du filtrage URL.

L'écran de la configuration globale

NetBios CIFS : liste des ports TCP par défaut

Cette liste contient les ports TCP autorisés par défaut pour NetBios CIFS.

Vous pouvez en ajouter en cliquant sur le bouton approprié, ou le retirer de la liste en le sélectionnant et en cliquant sur « Supprimer ».

NetBios CIFS : liste des ports UDP par défaut

Cette liste contient les ports UDP autorisés par défaut pour NetBios CIFS.
Vous pouvez en ajouter en cliquant sur le bouton approprié, ou le retirer de la liste en le sélectionnant et en cliquant sur « Supprimer ».

NetBios CIFS over SSL : liste des ports TCP par défaut

Cette liste contient les ports TCP autorisés par défaut pour le protocole NetBios CIFS passant par le SSL.
Vous pouvez en ajouter en cliquant sur le bouton approprié, ou le retirer de la liste en le sélectionnant et en cliquant sur « Supprimer ».

NetBios SSN

Les écrans sont les mêmes que pour le protocole précédent, à ceci près qu'ils permettent la configuration du protocole NetBios SSN, rendant possible l'échange de messages en mode connecté.

MGCP

L'écran des profils

Onglet « IPS »

Détecter et inspecter automatiquement le protocole	Si le protocole est activé, il est automatiquement utilisé à la découverte d'un paquet correspondant dans les règles de filtrage. Cette option n'est pas disponible pour les protocoles, IP, ICMP TCPUDP, RTP, RTCP, MSN, YMSG.

Paramètres de session MGCP

Taille max. d'une commande (octets)	Une commande peut comporter entre 32 et 1024 octets.
Nb max. de paramètres par commande	Le nombre de paramètres pouvant figurer au sein d'une commande doit être compris entre 32 et 1024 octets.
Taille max. du paramètre SDP (octets)	Le paramètre SDP valide automatiquement le lancement des applications dans une session depuis le *www* du client ou par la messagerie. Sa taille doit être comprise entre 32 et 1024 octets.
Durée d'inactivité max. (secondes)	La durée d'inactivité maximale d'une session doit être comprise entre 60 et 604800 octets.

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'action « passer » sera automatiquement déclenchée au sein du filtrage URL.

L'écran de la configuration globale

MGCP : liste des ports par défaut

Cette liste contient les ports autorisés par défaut pour le protocole MGCP.
Vous pouvez en ajouter en cliquant sur le bouton approprié, ou le retirer de la liste en le sélectionnant et en cliquant sur « Supprimer ».

RTP

Onglet « IPS »

Liste des codecs RTP supportés

Cette liste contient les codecs RTP supportés par défaut.
Vous pouvez en ajouter en cliquant sur le bouton approprié, ou le retirer de la liste en le sélectionnant et en cliquant sur « Supprimer ».

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'action « passer » sera automatiquement déclenchée au sein du filtrage URL.
Tracer chaque requête RTP	Active ou désactive les logs permettant de tracer les requêtes RTP.

RTCP

Onglet « IPS »

Commandes RTCP autorisées

Il est possible de définir des commandes RTCP au sein de la prévention d'intrusion, en cliquant sur **Ajouter**, dans la limite de 115 caractères. La suppression est également autorisée.

Commandes RTCP interdites

Il est possible d'interdire des commandes RTCP au sein de la prévention d'intrusion, dans la limite de 115 caractères.

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'action « passer » sera automatiquement déclenchée au sein du filtrage URL.
Tracer chaque requête RTCP	Active ou désactive les logs permettant de tracer les requêtes RTCP.

SIP

Le protocole SIP assure l'analyse protocolaire ainsi que l'autorisation dynamique des connexions secondaires. L'analyse des connexions est réalisée ligne par ligne: la ligne doit être complète avant le lancement de l'analyse. Pour chaque ligne d'en-tête une vérification est réalisée en fonction de l'état de l'automate.

- Pour les requêtes et les réponses :
Vérification de la version SIP et de l'opération, validation de l'URI qui doit être encodée en UTF-8.
  - Analyse de l'en-tête ligne par ligne: validation des champs de l'en-tête et extraction d'information (nom de l'appelant et de l'appelé ...), protection contre les attaques (encodage, débordement de tampons, présence et ordre des champs obligatoires, format des lignes ...).
  - Analyse et validation des données présentes dans le SDP (encodage, débordement de tampons, conformité à la RFC, présence et ordre des champs obligatoires, format des lignes ...).
- Pour les réponses (en plus des vérifications précédentes): cohérence générale de la réponse et cohérence par rapport à la requête.
La fonction d'audit est agrémentée d'un identifiant de groupe de session permettant de retrouver toutes les connexions d'une conversation, les noms de l'appelant et de l'appelé et le type de média utilisé (audio, vidéo, application, donnée, contrôle ...).

Détection automatique du protocole	Si le plugin est activé, il est automatiquement utilisé à la découverte d'un paquet correspondant dans les règles de filtrage. Cette option n'est pas disponible pour les protocoles IP, ICMP TCPUDP, RTP, RTCP, MSN, YMSG.

Commandes SIP

Commandes SIP autorisées

Ajouter	Insérer dans la liste des commandes additionnelles qui nécessitent une autorisation.
Supprimer	Sélectionnez la commande à retirer de la liste et cliquez sur **Supprimer**.

Commandes SIP interdites

Ajouter	Insérer dans la liste des commandes additionnelles qui ne sont pas autorisées.
Supprimer	Sélectionnez la commande à retirer de la liste et cliquez sur **Supprimer**.

Taille maximale des éléments (en octets)

Requête SIP [64-4096]	Taille maximale de la requête et de la réponse. Permet de gérer le débordement de mémoire.
En-tête SIP [64-4096]	Taille maximale de l'en-tête. Permet de gérer le débordement de mémoire.
Protocole SDP [64-604800]	Taille maximale d'une ligne SDP. Permet de gérer le débordement de mémoire.

Paramètres de session SIP

Nombre maximum de requêtes en attente [1-512]	Nombre maximum de requêtes sans réponses sur une même session SIP.
Durée de session (secondes) [60-604800]	Temps en secondes d'une session SIP.

Extension du protocole SIP

Activer l'extension INFO (RFC2976)	L'extension INFO permet d'échanger des informations lors d'un appel en cours. **Exemple** La puissance du signal wifi de l'un des deux correspondants. Cochez la case pour activer l'extension.
Activer l'extension PRACK (RFC3262)	Il existe deux types de réponses définies par SIP : les provisoires et les définitives. L'extension PRACK permet de fournir un système de reconnaissance fiable et de garantir une livraison ordonnée des réponses provisoires dans SIP. Cochez la case pour activer l'extension.
Activer l'extension SUSCRIBE, NOTIFY (RFC3265)	Le protocole SIP inclut un mécanisme normalisé pour permettre à n'importe quel client (un téléphone en VoIP étant un exemple de client SIP) de surveiller l'état d'un autre dispositif. Si un dispositif A client veut être informé des changements de statut d'un dispositif B, il envoie une requête SUBSCRIBE (de Souscription) directement au dispositif B ou à un serveur qui rend compte de l'état du dispositif B. Si la requête SUBSCRIBE est réussie, chaque fois que le dispositif B changera d'état, le dispositif A recevra un SIP NOTIFY, message indiquant le changement du statut ou présentant des informations sur l'événement. Lorsqu'un dispositif s'enregistre sur un autre, il sera informé dès qu'un événement survient. **Exemple** La mise en ligne des contacts qu'ils recherchent. Cochez la case pour activer l'extension.
Activer l'extension UPDATE (RFC3311)	L'extension UPDATE permet à un client de mettre à jour les paramètres d'une session avant qu'elle soit établie, comme l'ensemble des flux de médias et de leurs codecs. Cochez la case pour activer l'extension.
Activer l'extension MESSAGE (RFC3428)	L'extension MESSAGE est une prolongation du protocole SIP, permettant le transfert des messages instantanés. Puisque la requête MESSAGE est une prolongation au SIP, elle hérite de tous dispositifs de cheminement et de sécurité inclus dans ce protocole. Les requêtes MESSAGE portent le contenu au format de type MIME.

	Cochez la case pour activer l'extension.
Activer l'extension REFER (RFC3515)	L'extension REFER est utilisée notamment pour le transfert ou la redirection d'appels. Si un correspondant A essaie de joindre B et que ce dernier est indisponible, A sera redirigé vers un correspondant C, qui fait office de « référent » pour B. Cochez la case pour activer l'extension.
Activer l'extension PUBLISH (RFC3903)	L'extension PUBLISH permet de publier l'état des événements vers un destinataire. Cochez la case pour activer l'extension.
Activer le support pour le protocole PINT	Cette extension permet de faire coexister des téléphones SIP avec des services non IP (fax, etc.). Cochez la case pour activer l'extension.
Activer le support pour Microsoft Messenger (MSN)	Cette option permet d'activer le support de Microsoft Windows Messenger.

Support

Désactiver la prévention d'intrusion	En cochant cette option, l'action « passer » sera automatiquement déclenchée au sein du filtrage URL.
Tracer chaque requête SIP	Active ou désactive les logs permettant de tracer les requêtes SIP.

Autres

Cette partie est dédiée au « reste » des protocoles que vous pouvez rencontrer et non cités ci-avant.
L'écran est divisé en cinq colonnes :

Nom du protocole	Le nom donné au protocole.
Port par défaut	Le nom du port affecté par défaut : Il est possible de créer un nouveau port en cliquant sur l'icône à droite de la colonne.
Port SSL par défaut	Nom du port attribué au protocole par défaut.
Détection automatique	Vous pouvez choisir d'activer ou non la détection automatique du protocole : Tous les protocoles étant activés par défaut, double-cliquez sur la colonne pour désactiver la détection automatique du protocole concerné.
Etat	Vous pouvez choisir d'activer ou non le protocole sélectionné. Les protocoles étant activés par défaut, double-cliquez dans la colonne pour désactiver le protocole concerné. Répétez l'opération lorsque vous souhaitez le réactiver.

Cliquez sur le bouton « Appliquer » pour conserver vos modifications.

PROXY CACHE DNS

Lorsque vous effectuez une requête DNS vers votre navigateur ou vers une adresse mail, le serveur DNS transforme le nom de domaine connu (par exemple *www.netasq.com* ou *smtp.netasq.com*) en adresse IP et vous la communique.

Le Proxy cache DNS permet de stocker dans la mémoire du firewall, la réponse et l'adresse IP communiquée par le serveur au préalable. Ainsi, dès qu'une requête similaire sera effectuée, le firewall répondra à la place du serveur plus rapidement, et fournira l'adresse IP souhaitée et conservée.

L'écran du **Proxy cache DNS** se compose d'un écran unique, divisé en deux parties :

- Un tableau listant les clients DNS autorisés à utiliser le cache.
- Un menu déroulant permettant de définir les paramètres de la configuration avancée.

Activer le cache de requête DNS

Cette option permet de faire fonctionner le Proxy cache DNS : lorsqu'une requête DNS est envoyée au firewall, celle-ci est traitée par le cache DNS.

Liste des clients DNS autorisés à utiliser le cache

Client DNS [machine, réseau, plage, groupe] :

Les clients renseignés au sein de la liste peuvent émettre des requêtes DNS au travers du firewall.

Ajouter	En cliquant sur ce bouton, une nouvelle ligne vient se positionner en tête du tableau. La flèche située à droite du champ présenté vide permet d'ajouter un client DNS. Vous pouvez le sélectionner dans la base d'objets qui s'affiche. Cela peut être une machine, un réseau, une plage d'adresse ou encore un groupe.
Supprimer	Sélectionnez d'abord le client DNS que vous souhaitez retirer de la liste. Une fenêtre de confirmation s'affiche avec le message suivant : « **Supprimer le client DNS sélectionné** ? ». Vous pouvez valider la suppression ou **Annuler** l'action.



NOTE
En mode transparent, les clients sélectionnés bénéficieront du Proxy cache DNS, les autres demandes seront soumis au filtrage.

Configuration avancée

Taille du cache (octets) :

La taille maximale allouée au cache DNS dépend du modèle de votre firewall.

Mode transparent (intercepte toutes les requêtes DNS émise par les clients autorisées)	Comme son nom l'indique cette option vise à rendre transparent le service DNS du firewall NETASQ. Ainsi lorsque cette option est activée la redirection des flux DNS vers le cache DNS est invisible aux utilisateurs qui pensent accéder à leur serveur DNS. En mode transparent, toutes les requêtes sont interceptées, même si celles-ci sont à destination d'autres serveurs DNS que le firewall. Les réponses sont gardées un certain temps en mémoire pour éviter de retransmettre des demandes déjà connues.
Interrogation aléatoire des serveurs DNS	En cochant cette option, le firewall va sélectionner au hasard le serveur DNS dans la liste. (voir menu `Système`/module `Configuration`/onglet `Paramètres Réseaux`/panneau `Résolution DNS`).

QUALITE DE SERVICE (QoS)

L'écran de configuration de la qualité de service se compose d'un écran unique.

Trafic réseau

Un élément important dans la "Qualité de Service" est de résoudre le problème du niveau généralement très haut du taux de perte de paquets sur l'Internet. En effet lorsqu'un paquet est perdu avant d'atteindre sa destination, toutes les ressources mises en œuvre lors de son transit sont gâchées. Dans certain cas, cette situation peut même amener une situation de congestion grave qui parfois entraîne la paralysie totale des systèmes.
On est loin de la nécessité de stabilité et de "temps réel" des applications de vidéoconférence d'aujourd'hui. Le contrôle optimisé des situations de congestion et la gestion des queues de données deviennent un enjeu important de la "Qualité de Service".
Les firewalls NETASQ disposent de deux algorithmes pour leur traitement des congestions, l'algorithme **TailDrop** et l'algorithme **BLUE.** NETASQ recommande toutefois l'utilisation de l'algorithme BLUE comme algorithme de traitement des congestions.

Traitement en cas de saturation	Cette option permet de définir l'algorithme de traitements des congestions. Elle a comme objectif d'éviter les ralentissements.
File d'attente par défaut	Cette option permet de sélectionner, parmi les files d'attente définies, laquelle sera la file d'attente par défaut. Plus exactement, cette option permet de choisir la façon dont le trafic par défaut (qui ne correspond à aucune queue) sera traité par rapport au reste. Par défaut, ce trafic est prioritaire sur le trafic traité par la QoS (« Prioritaire sur tout »), mais il est possible de soumettre le trafic à une certaine queue, en la sélectionnant dans cette liste déroulante.

Réservation ou limitation de la bande passante (CBQ)

Bande passante totale	La valeur de référence en Kbits/s ou en Mbits/s permet d'indiquer une référence sur laquelle seront basées les limitations de bande passante indiquée en pourcentage dans la configuration des files d'attente.

A partir de la version 9.0.1, les paquets « ACK » et « low delay » DSCP sont maintenant traités avec une meilleure priorité par défaut (afin d'accélérer le transfert de données à travers une bande passante limitée).

Files d'attente

Le module de `QoS`, intégré au moteur de prévention d'intrusion NETASQ est associé au module `Filtrage` pour offrir les fonctionnalités de Qualité de Service.
Dès sa réception ; le paquet est traité par une règle de filtrage puis le moteur de prévention d'intrusion l'affecte à la bonne file d'attente suivant la configuration du champ QoS de cette règle de filtrage.
Il existe trois types de file d'attente sur le firewall. Deux sont directement associés aux algorithmes de QoS : PRIQ (Priority Queuing) et CBQ (Class-Based Queuing), le troisième type permet le monitoring du trafic.

File d'attente par classe d'application ou d'affectation (CBQ)

Il est possible de choisir une classe d'ordonnancement pour chacune des règles de filtrage et de lui associer une garantie de bande passante ainsi qu'une limite.
Par exemple; vous pouvez associer une classe d'ordonnancement aux flux http en associant une queue CBQ à la règle de filtrage correspondante.

Les files d'attente par classe d'application ou d'affectation induisent la façon dont les trafics affectés par ces règles de QoS seront gérés sur le réseau. Les mécanismes de réservation et de limitation de la bande passante de ce type de files d'attente permettent dans le premier cas, la garantie d'un service minimum et dans le deuxième cas, la préservation de la bande passante vis-à-vis d'applications coûteuses en ressources.

Ajout d'une file d'attente par classe d'application ou d'affectation

Pour ajouter une file d'attente par classe d'application ou d'affectation, cliquez sur le bouton **Ajouter une file d'attente**, puis sélectionnez **Réservation ou limitation de bande passante (CBQ).** Une ligne est ajoutée à la grille dans laquelle vous pouvez effectuer vos modifications.

Modification d'une file d'attente par classe d'application ou d'affectation

Nom	Nom de la file d'attente à configurer.
Type	Type de file d'attente parmi **CBQ**, **PRIQ** ou **MONQ**).
Priorité	Permet de choisir le niveau de priorité du trafic affecté à la queue. Les cellules de cette colonne ne sont éditables que pour les queues de type PRIQ. Il est possible de sélectionner une valeur allant de 7 (priorité la plus faible) à 1 (priorité la plus haute).
Bp min	Agissant comme une garantie de service, cette option permet la garantie d'un débit donné et d'un délai maximal de transfert. Configurée en Kbits/s ou en pourcentage de la valeur de référence, cette valeur est partagée entre tous les trafics affectés par la règle de QoS. Ainsi si les trafics HTTP et FTP sont associées à une file d'attente qui possède un minimum garanti de 10Kbits/s alors la bande passante HTTP + la bande passante FTP sera au minimum de 10Kbits/s. Cependant rien n'empêche que la bande passante HTTP soit de 9Kbits/s et la bande passante soit seulement de 1Kbit/s. **REMARQUE** Par défaut, cette option est synchronisée avec l'option **Min inv**. En modifiant la valeur de cette option, la réplication de cette valeur est réalisée dans **Min inv**. En modifiant la valeur de **Min inv**, les valeurs sont différentes et donc désynchronisées.

Bp max	Agissant comme une limitation, cette option interdit le dépassement de bande passante pour le trafic affecté par ces files d'attente. Configurée en Kbits/s, en Mbits/s, en Gbit/s ou en pourcentage de la valeur de référence, cette valeur est partagée entre tous les trafics affectés par la règle de QoS. Ainsi si les trafics HTTP et FTP sont associées à une file d'attente qui possède un maximum autorisé de 500Kbits/s alors la bande passante HTTP + la bande passante FTP ne doit pas dépasser 500Kbits/s.  **REMARQUE** Par défaut, cette option est synchronisée avec l'option **Max inv**. En modifiant la valeur de cette option, la réplication de cette valeur est réalisée dans **Max inv**. En modifiant la valeur de **Max inv**, les valeurs sont différentes et donc désynchronisées.
Min inv.	Agissant comme une garantie de service, cette option permet la garantie d'un débit donné et d'un délai maximal de transfert. Configurée en Kbits/s ou en pourcentage de la valeur de référence, cette valeur est partagée entre tous les trafics affectés par la règle de QoS. Ainsi si les trafics HTTP et FTP sont associées à une file d'attente qui possède un minimum garanti de 10Kbits/s alors la bande passante HTTP + la bande passante FTP sera au minimum de 10Kbits/s. Cependant rien n'empêche que la bande passante HTTP soit de 9Kbits/s et la bande passante soit seulement de 1Kbit/s.  **REMARQUE** Si vous saisissez une valeur supérieure à **Max inv.**, dans ce cas le message suivant s'affiche : « *trafic descendant : La bande passante minimale garantie doit être inférieure ou égale à la bande passante maximale* ».
Max inv.	Agissant comme une limitation, cette option interdit le dépassement de bande passante pour le trafic descendant, affecté par ces files d'attente. Configurée en Kbits/s, en Mbits/s, en Gbit/s ou en pourcentage de la valeur de référence, cette valeur est partagée entre tous les trafics affectés par la règle de QoS. Ainsi si les trafics HTTP et FTP sont associées à une file d'attente qui possède un maximum autorisé de 500Kbits/s alors la bande passante HTTP + la bande passante FTP ne doit pas dépasser 500Kbits/s.
Couleur	Couleur de différentiation de la file d'attente.
Commentaire	Commentaire associé.

 **REMARQUE**

Lorsque vous sélectionnez 0 dans la colonne « Bpmin » et Illimité dans la colonne « Bp max », aucune contrainte n'est imposée sur le trafic. Dans ce cas, un message s'affiche dans lequel l'application vous propose de transformer votre file d'attente par une file de surveillance.

La grille du menu `File d'attente par classe d'application ou d'affectation` affiche les différentes files d'attente qui ont été configurées. Un clic sur le bouton **Vérifier l'utilisation** permet d'afficher (dans la barre de navigation à gauche, la liste des règles de filtrage dans lesquelles la file d'attente sélectionnée est utilisée.)

Suppression d'une file d'attente par classe d'application ou d'affectation

Sélectionnez la ligne de file d'attente à supprimer puis cliquez sur le bouton **Supprimer**. Un message s'affiche vous demandant si vous souhaitez réellement supprimer la file d'attente.

Surveillance du trafic (monitoring)

Les files d'attente de monitoring n'affectent pas la manière dont sont traités les trafics qui sont associés à ces règles de QoS. Elles permettent l'enregistrement d'informations de débit et de bande passante qui peuvent être visualisées au moyen de NETASQ EVENT REPORTER, dans l'onglet **`Graphiques`** du logiciel.
Les différentes options de la configuration d'une file d'attente du type Monitoring sont présentées ci-dessous :

Ajout d'une surveillance du trafic

Pour ajouter une surveillance du trafic, cliquez sur le bouton **Ajouter** une file d'attente puis sélectionnez **Surveillance du trafic (MONQ).**

Modification d'une surveillance du trafic

Nom	Nom de la file d'attente à configurer.
Type	Type de file d'attente parmi **CBQ**, **PRIQ** ou **MONQ**.
Couleur	Couleur de différenciation de la file d'attente.
Commentaire	Commentaire associé.

Suppression d'une surveillance du trafic

Sélectionnez la ligne concernée dans la grille de surveillance de trafic puis cliquez sur le bouton **Supprimer**. Un message s'affiche vous demandant si vous souhaitez réellement supprimer la file d'attente.

File d'attente par priorité

Il existe 7 niveaux de priorité. Les paquets seront traités en fonction des priorités paramétrées.
Il est possible d'associer une priorité élevée aux requêtes DNS en créant une règle de filtrage et en lui associant une queue PRIQ.

Les files d'attente par priorité induisent une priorisation des paquets dans leur traitement. Les paquets qui sont associés à une règle de filtrage avec une file d'attente du type **PRIQ** sont traités avant les autres.
Les priorités s'échelonnent entre 1 et 7. La priorité 1 correspond aux trafics les plus prioritaires parmi les files d'attente **PRIQ**. La priorité 7 correspond aux trafics les moins prioritaires parmi les files d'attente **PRIQ**. Les files d'attente **CBQ** et les flux sans règles de QoS sont associés à une priorité 8 "virtuelle" (elle n'est pas configurable) qui définit que quoi qu'il arrive, ces flux seront traités après toutes files d'attente du type **PRIQ**.
Les différentes options de la configuration d'une file d'attente du type PRIQ sont présentées ci-dessous.

Ajout d'une file d'attente par priorité

Pour ajouter une file d'attente par priorité, cliquez sur le bouton **Ajouter une file d'attente**, puis sélectionnez **Traitement par priorité (PRIQ).**
Une ligne est ajoutée à la grille dans laquelle vous pouvez effectuer vos modifications.

Modification d'une file d'attente par priorité

La grille affiche les différentes files d'attente qui ont été configurées. Il est possible de vérifier si ces règles sont utilisées dans une règle de filtrage en cliquant sur le bouton **Vérifier l'utilisation**. Dans ce cas, un menu apparaît dans la barre de navigation en affichant les règles.

Nom	Nom de la file d'attente à configurer.
Type	Type de file d'attente parmi **CBQ**, **PRIQ** ou **MONQ**.
Priorité	Permet de choisir le niveau de priorité du trafic affecté à la queue. Les cellules de cette colonne ne sont éditables que pour les queues de type PRIQ. Il est possible de sélectionner une valeur allant de 7 (priorité la plus faible) à 1 (priorité la plus haute).
Couleur	Couleur de différenciation de la file d'attente.
Commentaire	Commentaire associé.

Suppression d'une file d'attente par priorité

Sélectionnez la ligne concernée dans la grille de file d'attente par priorité puis cliquez sur le bouton **Supprimer**. Un message s'affiche vous demandant si vous souhaitez réellement supprimer la file d'attente.

Files d'attente disponibles

A la fin de la grille des files d'attente est indiqué le nombre de files d'attentes disponibles pour un modèle de firewall donné (20 pour les U30 et U70, 100 pour les U120, U250 et U450, 200 pour les U1100, U1500 et NG1000-A, 255 pour le U6000 et le NG5000-A).

Cas d'application et recommandations d'utilisation

Exemple 1 : Priorisation des flux DNS

Basées sur UDP, les requêtes DNS subissent de nombreuses pertes de paquets du fait de la définition même du protocole UDP. Celui-ci ne prévoit pas de mécanismes de gestion des erreurs de transmission et l'écrasante présence des trafics TCP noient les trafics UDP dans la masse des paquets TCP.

Pour préserver ces trafics, et en particulier les flux DNS, il est recommandé de prévoir une règle de QoS de type "priorité" (PRIQ). Elle permettra de diminuer les trop fréquentes pertes de paquets et la latence qu'il pourrait y avoir sur ce type de trafic qui demande une réactivité importante (c'est d'ailleurs pour cette raison que les requêtes DNS sont réalisées sur UDP).

Définition de la règle de QoS pour le DNS

Nom	Type	Priorité	Bp min	Bp max	Min inv.	Max inv.	Couleur	Commentaire
File d'attente par priorité (1 Item)								
QoS_DNS		**1**						**Priorisation flux DNS**

Utilisation de la règle de QoS dans la politique de filtrage

Afin de visualiser la `QoS` dans l'onglet `Filtrage`, du module `Filtrage et NAT`, double-cliquez dans la colonne **Action** une fois votre règle de filtrage établie (voir document *Filtrage et NAT* ou menu `Politique de Sécurité`\module `Filtrage et NAT`\colonne Action).

Effets sur le trafic

- Baisse voire absence de paquets perdus si la règle est en priorité 1 (et qu'elle est la seul dans ce cas).
- Diminution de la latence.

Exemple 2 : Limitation du trafic HTTP

Parmi les trafics internet, les flux HTTP sont les plus gros consommateurs de la bande passante du lien Internet et du réseau local. Une utilisation importante de l'internet peut entraîner des problèmes de congestions du trafic réseau, les performances globales sont dégradées et l'utilisation du réseau devient fastidieuse.

Pour remédier à cet état de fait, il est recommandé de **limiter le trafic HTTP au moyen d'une règle de QoS de type "classe d'application ou d'affectation" (CBQ) définissant un débit maximum autorisé**. Elle permettra de préserver la bande passante du réseau et réduire l'impact de l'utilisation de l'internet sur les performances globales du réseau.

Définition de la règle de QoS pour le HTTP

Nom	Type	Priorité	Bp min	Bp max	Min inv.	Max inv.	Couleur	Commentaire
File d'attente par classe d'application ou d'affectation (1 Item)								
QoS_HTTP			**0kb**	**512kb**	**0kb**	**512kb**		**Limitation trafic HTTP**

Utilisation de la règle de QoS dans la politique de filtrage

Afin de visualiser la `QoS` dans l'onglet `Filtrage`, du module `Filtrage et NAT`, double-cliquez dans la colonne **Action** une fois votre règle de filtrage établie (voir document *Filtrage et NAT* ou menu `Politique de Sécurité`\module `Filtrage et NAT`\colonne Action).

Effets sur le trafic

- Diminution du risque de congestion du réseau.
- Réduction de l'impact du trafic sur les performances générales du réseau.

Exemple 3 : Garantie d'un niveau de service minimum

Certaines applications (VoIP par exemple) nécessitent un niveau de services avec la garantie que ce niveau de services sera respecté sous peine de disfonctionnement du service (impossibilité de suivre une conversation VoIP par exemple). Les autres applications et leur impact sur les performances générales du réseau peuvent perturber l'obtention du niveau de services requis.

Pour s'assurer que le niveau de services requis sera maintenu il est recommandé de créer une règle de QoS de type "classe d'application ou d'affectation" (CBQ) définissant un débit minimum garanti. Elle permettra de garantir un niveau de service pour un trafic donné indépendamment de l'impact des autres trafics sur les performances globales du réseau et sans définir de limitation de bande passante pour ces autres trafics.

Définition de la règle de QoS pour la VoIP

Nom	Type	Priorité	Bp min	Bp max	Min inv.	Max inv.	Couleur	Commentaire
File d'attente par classe d'application ou d'affectation (1 Item)								
QoS_VoIP			**1kb**	**0kb**	**100kb**	**0kb**		**Garantie service minimum**

Utilisation de la règle de QoS dans la politique de filtrage

Afin de visualiser la `QoS` dans l'onglet `Filtrage`, du module `Filtrage et NAT`, double-cliquez dans la colonne **Action** une fois votre règle de filtrage établie (voir document *Filtrage et NAT* ou menu `Politique de Sécurité`\module `Filtrage et NAT`\colonne Action).

Effets sur le trafic

- Garantie d'une bande passante pour un trafic donné.
- Introduction d'un temps de réponse maximal pour le transfert des données du service.

REGLES IMPLICITES

Règles de filtrage implicites

Cet écran vous informe qu'il est possible de générer automatiquement différentes règles de filtrage IP pour autoriser l'utilisation des services du firewall. Si vous activez un service, le firewall crée de lui-même les règles de filtrage nécessaires, sans avoir besoin de créer des règles « explicites » dans la politique de filtrage.

La grille de règles

La grille présente les colonnes suivantes :

Activé	Etat de la règle : **Activé**/ **Désactivé** : Cliquez dans la case pour activer/désactiver la création d'une ou plusieurs règles implicites. La règle **Autoriser l'accès au portail d'authentification et au VPN SSL pour les interfaces externes (non protégées (Auth_ext)** est désactivée par défaut.
Nom	Nom de la règle implicite : celui-ci n'est pas modifiable.

Les règles suivantes figurent dans la colonne « **Nom** » :

- **Autoriser l'accès au portail d'authentification et au VPN SSL pour les interfaces externes (non protégées) (Auth_ext)** : une règle autorisant l'accès au service https (port 443) est créée pour chaque interface externe (publique). Les utilisateurs peuvent donc s'authentifier et accéder au VPN SSL depuis les réseaux externes.
- **Autoriser l'accès au portail d'authentification et au VPN SSL pour les interfaces protégées (Authd_int)** : une règle autorisant l'accès au service https (port 443) est créée pour chaque interface interne (protégée). Les utilisateurs peuvent donc s'authentifier et accéder au VPN SSL depuis les réseaux internes.
- **Bloquer et réinitialiser les requêtes ident (port 113) pour les interfaces modems (dialup)**.
- **Bloquer et réinitialiser les requêtes ident (port 113) pour les interfaces ethernet**.
- **Autoriser l'accès au service DNS (port 53) du Firewall pour les interfaces protégées** : les utilisateurs peuvent joindre service DNS, et donc utiliser le proxy cache DNS, si ce dernier est activé.
- **Autoriser l'accès mutuel entre les membres d'un groupe de firewalls (cluster H.A)** : cela permet aux différents membres du cluster HA de communiquer entre eux.
- **Autoriser l'accès au serveur PPTP** : les utilisateurs peuvent contacter le firewall via le protocole PPTP pour accéder au serveur, s'il est activé.

- **Autoriser l'accès au serveur d'administration (port 1300) du firewall pour les interfaces protégées (Serverd)** : les administrateurs pourront se connecter via les réseaux internes sur le port 1300 du firewall. Ce service est utilisé notamment par le NETASQ Real-Time Monitor.

- **Autorise l'accès au port ssh du Firewall pour les interfaces protégées**: permet d'ouvrir l'accès au firewall par SSH afin de pouvoir se connecter dessus en lignes de commande à partir d'une machine située sur les réseaux internes.
- **Autoriser ISAKMP (port 500 UDP) et le protocole ESP pour les correspondants VPN IPSec** :
  Les correspondants VPN IPSec pourront contacter le firewall via ces deux protocoles permettant de sécuriser les données circulant sur le trafic IP.
- **Autoriser l'accès au serveur d'administration (port 443) du Firewall pour les interfaces protégées (WebAdmin)** : les administrateurs pourront se connecter via les réseaux internes sur le port 443, utilisé par l'interface d'administration web.

NOTE
Cette règle autorise l'accès au portail captif, et donc à l'interface d'administration web pour tous les utilisateurs connectés depuis une interface protégée. Pour restreindre l'accès à l'administration web (répertoire « /admin/ »), il faut indiquer une ou plusieurs machines depuis l'écran `Système \ Configuration \ onglet Administration du Firewall`. Un tableau permet de restreindre l'accès à ces pages au niveau applicatif web.

AVERTISSEMENTS
Deux cas peuvent être dangereux :

- **Désactiver la règle « Serverd »** : peut amener, en cas d'absence de règle explicite, à ne plus avoir d'accès avec les outils utilisant le port 1300, à savoir NETASQ RealTime Monitor, GlobalAdmin, NETASQ Event Reporter, NETASQ Centralized Management et NETASQ Event Analyzer.

- **Désactiver la règle « WebAdmin »** : vous n'aurez plus accès à l'interface d'administration web, sauf si une règle explicite l'autorise.

ROUTAGE

Le fonctionnement du routage est segmenté en deux parties :

- `Passerelle` : 2 configurations sont possibles ici. Une configuration simple dans laquelle il suffit d'indiquer une passerelle par défaut ; pour utiliser plusieurs passerelles, il faut utiliser la configuration avancée.

  Cet onglet permet donc la définition de la route par défaut, la définition des passerelles principales et de secours ainsi que la configuration de la répartition de charge. L'onglet **`Passerelle`** peut être considéré comme une forme avancée de la route par défaut. Il propose une utilisation simultanée de plusieurs routes pour acheminer un paquet, suivant un algorithme paramétrable. L'onglet **`Passerelle`** fonctionne avec un système de secours (backup).
- `Routage statique` : Permet la définition des routes statiques. Le routage statique représente un ensemble de règles définies par l'administrateur ainsi qu'une route par défaut.

Ces deux parties fonctionnent simultanément, le routage statique étant prioritaire sur tout le reste lors de l'acheminement d'un paquet sur le réseau.

L'onglet « Passerelle »

Passerelle par défaut (routeur)	Le routeur par défaut est généralement l'équipement qui permet l'accès de votre réseau à Internet. C'est à cette adresse que le firewall NETASQ envoie les paquets qui doivent sortir sur le réseau public. Bien souvent le routeur par défaut est connecté à l'Internet. Si vous ne configurez pas le routeur par défaut, le firewall NETASQ ne sait pas laisser passer les paquets possédant une adresse de destination différente de celles directement reliées au firewall. Vous pourrez communiquer entre les machines sur les réseaux internes, externes ou DMZ, mais aucun autre réseau (dont Internet). Cliquer sur le bouton permet d'accéder à la base d'objets et de sélectionner une machine. Une fois la sélection faite, le nom de la machine réapparaît sur l'écran. Cette option peut être grisée dans le cas où plusieurs passerelles principales sont définies.

Configuration avancée

Le firewall permet d'effectuer un routage réparti entre plusieurs passerelles principales avec tolérance de panne. Pour choisir la répartition, sélectionnez l'une des options ci-dessous :

Répartition de charge	3 options sont disponibles :"En fonction de l'adresse source", "En fonction de la source et de la destination (connexion) ", et "Aucune répartition". - **En fonction de l'adresse source** : Toutes les routes définies dans la

grille "Liste des passerelles utilisées" sont utilisées. Un algorithme permet de répartir le routage en fonction de la source qui est à l'origine du trafic routé. Si trop de routes principales tombent en panne, le lot des routes de secours prend le relai, à la condition que le module de haute disponibilité soit activé.

- **En fonction de la source et de la destination (connexion)** : Le partage est presque identique au partage de charge par source sauf que l'algorithme de partage se base également sur la destination du trafic. Pour résumer, selon une machine définie, suivant ses connexions, les paquets ne passeront pas nécessairement par la même route.
- **Aucune répartition** : La première route définie dans les grilles "Liste des passerelles utilisées" et "Liste des passerelles de secours", est utilisée pour le routage tandis que les autres sont ignorées. Donc, si la route principale tombe en panne, la route de secours prend le relai (si elle existe).



REMARQUE

Les commandes sont passées en temps réel lors du choix du partage de charge. S'il y a échec, alors les boutons radio sont restaurés.

Les boutons d'action

Pour pouvoir ajouter ou supprimer des routes, cliquez sur le bouton **Ajouter** ou le bouton **Supprimer**.

Ajouter	Permet d'ajouter une passerelle principale ou de sauvegarde. Un clic sur ce bouton ajoute une ligne à la fin de la grille.
Supprimer	Permet de supprimer une passerelle ou plusieurs passerelles simultanément.
Déplacer dans la liste de secours/Déplacer dans la liste principale	Permet de basculer une route de la grille principale à la grille de secours ou de la grille de secours à la grille principale.
Monter	Permet de faire remonter dans la grille la passerelle sélectionnée afin que celle-ci devienne prioritaire.
Descendre	Permet de faire redescendre dans la grille la passerelle sélectionnée afin que celle-ci ait une priorité moindre.

Passerelles principales et de secours

Les grilles pour les passerelles principales et les passerelles de secours comportent les colonnes ci-dessous :

Passerelle (objet machine) (Obligatoire)	Objet de type « Machine » désignant son IP qui fait office de route. Cet objet peut être une machine quelconque ou une passerelle de dialup (Firewall_<nom_interface_dialup>_peer). Le nombre maximum de passerelles principales et de secours est de 16 (8 pour chaque). Si plus d'une passerelle principale est définie, l'option **Passerelle par défaut (routeur)** est désactivée.
Equipement(s) pour tester la disponibilité	Machine ou groupe de machines à tester (ping) afin de définir la connectivité de la passerelle. Ce test est fonctionnel à la condition que l'option **Activer la haute disponibilité de liens** soit cochée.
Commentaire	Commentaire concernant la passerelle.

Activer la Haute disponibilité de liens	Lorsque vous activez cette option, la Haute Disponibilité des routes est activée. Exemple : Imaginons que vous ayez 5 routes principales configurées et un seuil de basculement de 4. Si les 4 routes principales ne sont plus praticables, alors les routes de secours sont utilisées. Cette option permet également de rendre fonctionnel le test **Equipement pour tester la disponibilité.**
Seuil de basculement	Si on active la HA, alors, les passerelles de sauvegarde ne seront sollicitées que si le nombre de passerelles principales est inférieur au minimum de passerelles définies dans le champ **Seuil de basculement**. Ce nombre doit être au minimum de 1.

Envoi de la configuration

Les modifications effectuées sur cet écran sont validées à l'aide du bouton **Appliquer**. Une vérification de la cohérence des routes statiques est effectuée au préalable.

Si la configuration effectuée dans cet onglet présente deux passerelles principales, dans ce cas, le bouton de l'onglet `Passerelle` "Passerelle par défaut (routeur)" est grisé.

L'onglet « Routage statique »

Cet onglet correspond à la liste des routes statiques dont le nombre maximum varie selon le modèle :

U30	U70	U120	U250	U450	U1100	U1500	U6000	NG1000-A	NG5000-A
512	512	2048	2048	2048	5120	5120	10240	5120	10240

Présentation de la barre de boutons

Recherche	Recherche qui porte sur un objet machine, un réseau ou un groupe.
Ajouter	Ajoute une route statique "vide". L'ajout de la route (envoi de commande) devient effectif une fois la nouvelle ligne éditée et les champs **Réseau source (objet machine, réseau ou groupe)** et **Interface** remplis.
Supprimer	Supprime une route ou plusieurs routes préalablement sélectionnée(s). Utiliser les touches **Ctrl/Shift** + **Supprimer** pour la suppression de plusieurs routes.

Appliquer	Envoie la configuration des routes statiques.
Annuler	Annule la configuration des routes statiques.

Présentation de la grille

La grille présente six informations :

Réseau source (objet machine, réseau ou groupe) (Obligatoire)	Un clic sur cette colonne ouvre la base d'objets afin de sélectionner une machine, un réseau ou encore un groupe.
Plan d'adressage	Adresse IP ou groupe d'adresses liés aux éléments de la colonne « Réseau source (objet machine, réseau ou groupe) ».
Interface (Obligatoire)	Une liste déroulante permet de sélectionner une interface parmi Ethernet, Vlan, dialup.
Protégée	Cette colonne vous informe de la nature protégée ou pas de la route. Une route protégée est ajoutée à l'objet Network internals. Le comportement de la configuration de sécurité prendra en compte ce paramètre. Les machines joignables par cette route seront mémorisées dans le moteur de prévention d'intrusion.
Passerelle (Optionnel)	Un clic sur cette colonne ouvre la base d'objets afin de sélectionner une machine (routeur).
Couleur (Optionnel)	Une fenêtre s'affiche permettant de sélectionner une couleur d'interface (utilisée dans NETASQ REALTIME MONITOR et NETASQ EVENT REPORTER).
Commentaire (Optionnel)	Texte libre.

SERVEUR PPTP

L'écran de configuration du **serveur PPTP** se divise en 2 zones :

- **Configuration générale** : Activation du serveur PPTP, choix du pool d'adresses.
- **Configuration avancée** : Choix du nombre de connexions PPTP.

La mise en place est très simple et rapide. Elle se déroule en trois étapes :
Cet écran permet la configuration des paramètres suivants :

- Les adresses IP des clients PPTP (objet).
- Les paramètres de chiffrement.
- Le Serveur DNS et le serveur WINS.

Configuration générale

Activer le serveur PPTP	Activation/Configuration du serveur **PPTP** sur le firewall. Cela est réalisé en cochant **Activer le serveur PPTP**.
Adresses IP des clients PPTP (objet) (Obligatoire)	Une fois le serveur PPTP activé, il faut obligatoirement créer un pool d'adresses IP privées. Le firewall affecte au client qui vient se connecter en **PPTP** une adresse IP disponible dans le pool. Il faut créer un groupe de machines contenant les adresses réservées, ou une plage d'adresses provenant de la base objets.

Paramètres transmis aux clients PPTP

Serveur DNS	Le champ **Serveur DNS** permet d'envoyer l'adresse IP du serveur DNS au client.
Serveur WINS	Le champ **Serveur WINS** permet d'envoyer au client l'adresse IP du serveur WINS du site.

A partir de la version 9.0.1, les caractères « _ », « - », et « . » sont autorisés pour les noms des utilisateurs PPTP.

Configuration avancée

Nombre de connexions PPTP réservées [0-96] (nombre variable selon le modèle installé) : Si vous souhaitez créer un nouveau serveur PPTP et que vous êtes arrivé au maximum du nombre dynamique de PPTP possible, vous avez la possibilité d'en augmenter le nombre.



Dès qu'une modification est faite sur le nombre de connexions PPTP (diminution ou augmentation), un redémarrage est nécessaire pour prendre en compte cette modification.

Chiffrement du trafic

Les paramètres de chiffrement possibles sont :

Ne pas chiffrer	Désactive le champ **Accepter uniquement le trafic chiffré et autoriser les algorithmes suivants** ainsi que les MPPE proposés.
Accepter uniquement le trafic chiffré et autoriser les algorithmes suivants	Autorise la connexion uniquement si le client chiffre les données.
MPPE40 bits	Autorise l'utilisation du protocole de chiffrement MPPE 40 bits.
MPPE56 bits	Autorise l'utilisation du protocole de chiffrement MPPE 56 bits.
MPPE128 bits	Autorise l'utilisation du protocole de chiffrement MPPE 128 bits.

TABLEAU DE BORD

Le tableau de bord présente une vue d'ensemble des informations concernant votre firewall Il est représenté par cette icône  et est divisé en 2 parties :

- Le menu de configuration des modules à gauche, contenant 4 onglets dépliables et personnalisables selon vos besoins : « Mes favoris », « Configuration », « Objets », « Utilisateurs et groupes ». Une barre de recherche est disponible pour les 3 derniers modules cités.
- Une zone dynamique au centre, contenant 9 modules ou widgets :

Réseau
Alarmes
Ressources
Licence
Matériel
Propriétés
Active Update
Service
Interfaces

Par défaut, chacune des fenêtres est mise à jour dynamiquement, les composants les plus récents sont téléchargés automatiquement et s'affichent à l'écran.

Le menu de configuration des modules

Cette colonne rétractable (bouton «) est divisée en 4 rubriques déroulantes. Elles vous permettront de personnaliser votre interface et de configurer vos modules.

Mes favoris

Cette rubrique est étroitement liée à l'icône « épingle » : .
Lorsque vous rencontrez cette icône en haut à droite de chaque module, cochez-là si vous souhaitez qu'il fasse partie de vos favoris.

Configuration

Cette rubrique est représentée sous forme d'une arborescence de menus et de leurs modules, supplantée par une barre de recherche par mots clés.
9 menus sont disponibles (cliquez dessus afficher leur liste déroulante) :

- Tableau de bord
- Système (contenant 7 modules : Configuration, Administrateurs, Licence, Maintenance, Active Update, Haute disponibilité, Console cli)
- Réseau (contenant 5 modules : Interfaces, Routage, DNS Dynamique, DHCP, Proxy cache DNS)
- Objets (contenant 4 modules : Objets réseaux, Objets web, Certificats et PKI, Objets temps)
- Utilisateurs (contenant 5 modules : Utilisateurs, Droits d'accès, Configuration de l'annuaire, Authentification, Enrôlement)

- Politique de sécurité (contenant 6 modules : Filtrage et NAT, Filtrage URL, Filtrage SSL, Filtrage SMTP, Qualité de service, Règles implicites)
- Protection applicative (contenant 6 modules : Alarmes, Protocoles et Applications, Profils d'inspection, Détection de vulnérabilités, Antivirus, Antispam)
- VPN (contenant 3 modules : VPN IPSec, VPN SSL, Serveur PPTP)
- Notifications (contentant 5 modules : Traces syslog, Agent SNMP, Alertes e-mails, Evénements systèmes, Message de blocage)



Si vous rencontrez des modules grisés, cela signifie qu'ils nécessitent une licence à laquelle vous n'avez pas souscrit, et donc, que vous n'y avez pas accès.

Cela peut également signifier que l'utilisateur avec lequel vous vous êtes connecté n'a pas les privilèges nécessaires à l'accès de ces menus

L'icône » permet de personnaliser l'affichage de votre arborescence :

Ceci offre une visibilité partielle de votre arborescence, affichant uniquement les menus.

Cela offre une visibilité totale de votre arborescence, affichant les menus et leurs modules.

La zone dynamique : les widgets

Cet espace vous permet de visualiser certaines mises à jour de votre firewall comme les dernières alarmes remontées ou les dates d'expiration de vos licences.
9 fenêtres sont accessibles, disposant chacune d'une barre d'outils en haut à droite, y compris le module tableau de bord complet.
Les actions possibles via ces outils sont les suivantes :

« Plus »	Représenté par l'icône +, cet outil permet pour le module tableau de bord, d'ajouter une colonne, et pour les widgets, d'agrandir la fenêtre.
« Moins »	Représenté par l'icône -, cet outil permet pour le module tableau de bord, de supprimer une colonne, et pour les widgets, de réduire la fenêtre.
« Fermer »	Représenté par l'icône ✕, cet outil permet de fermer votre widget.
« Rafraîchir »	Représenté par l'icône , cet outil permet le rafraîchissement des données du tableau de bord ou du widget concerné.
« Ouvrir »	Représenté par l'icône , cet outil ouvre le module associé au widget sur lequel vous vous trouvez, et provoque de ce fait, la fermeture du tableau de bord.
« Configuration du tableau de bord »	Représenté par l'icône , cet outil vous permet de sélectionner les **Composants** que vous souhaitez voir apparaître sur le tableau de bord, via un système de coche. Vous pouvez également paramétrer la **Fréquence de mise à jour** des widgets : « Manuel uniquement » (vous devrez systématiquement cliquer sur l'icône « Rafraîchir » ( )) , « Toutes les minutes » ou « Toutes les 5 minutes ».
« Ajouter aux favoris »	Représenté par l'icône , cet outil permet d'ajouter le module `Tableau de bord` à votre rubrique « **Mes favoris** » au sein de l'arborescence de gauche (voir partie *Le menu de configuration des modules*).

Réseau

Cette fenêtre affiche le modèle de votre firewall multifonction NETASQ ainsi que le nombre d'interfaces disponibles sur celui-ci (32 maximum).
Le ou les interfaces utilisées apparaissent en vert et une info bulle contenant les informations de chacune d'entre elles est disponible.
Ces informations sont les suivantes :

Nom	Nom de l'interface utilisée (de type « in », « out » ou « dmz »), accompagné de son adresse IP et de son masque de sous-réseau.
Paquets réseaux	Le nombre de paquets Accepté, Bloqué, Fragmenté, TCP, UDP et ICMP.
Trafic reçu	La totalité et le détail des paquets TCP, UDP et ICMP reçus.
Trafic émis	La totalité et le détail des paquets TCP, UDP et ICMP émis.
Débit	Les débits entrant et sortant actuels.

Alarmes

Cette fenêtre contient la liste des 50 dernières alarmes levées par le firewall.

Date	La date et l'heure des dernières alarmes remontées, classée de la plus à la moins récente.
Priorité	3 niveaux de priorités sont possibles et configurables au sein du module `Protection Applicative/Alarmes`.
Source	Paquet IP ou connexion à l'origine du déclenchement de l'alarme.
Destination	Adresse visée par la source avant de déclencher l'alarme.
Message	Commentaire associé à l'alarme sélectionnée. **Exemples de messages possibles** « *Message ICMP invalide (no TCP/UDPlinked entry)* » (priorité type mineur). « *Usurpation d'adresse IP (type=1)* » (priorité type majeur).
Aide en ligne	Sélectionnez l'alarme voulue, et cliquez sur ce lien qui vous mènera à une page d'aide concernant le message (voir ci-dessus).
Action	Lorsqu'une alarme est remontée le paquet qui a provoqué cette alarme subit l'action associée. Les actions sont « Bloquer » ou « Passer ».

A partir de la version 9.0.1, cette partie du tableau de bord contient un nouveau bouton ( ) permettant de « Vider l'écran », c'est-à-dire d'effacer les journaux d'informations.

Ressources

Cette fenêtre donne une vue graphique des ressources matérielles relatives à votre firewall.

Espace utilisé	Espace utilisé pour les logs du firewall, en pourcentage.
CPU	Pourcentage d'utilisation de votre processeur.
Température	Température de votre équipement. Celle-ci n'est pas disponible sur machine virtuelle.

Mémoire	Mémoire utilisée par votre équipement : **Machine** : pourcentage de la mémoire allouée par les machines (octets). **Fragmenté** : pourcentage de la mémoire allouée par les fragments (ou dossiers trop lourds découpés en plusieurs morceaux- en octets). **Connexion** : pourcentage de la mémoire allouée pour les connexions diverses (octets). **ICMP** : pourcentage de la mémoire allouée pour le protocole ICMP (octets). **Traces** : pourcentage de la mémoire utilisée pour le DataTracking (suivi des données). **Dynamique** : mémoire informatique dans laquelle un ordinateur place les données lors de leur traitement.

Licence

Cette fenêtre affiche les différentes valeurs de votre licence et leur date limite de mise à jour.

Update	Date limite de mise à jour du boîtier.
Pattern	Date d'expiration des modèles ASQ.
Antivirus	Date limite de mise à jour des bases virales ClamAV et Kaspersky.
VulnBase	Date limite de mise à jour des vulnérabilités NVM (NETASQ Vulnerability Manager).
VirusVendor	Date limite de mise à jour des bases virales Kaspersky.
URLFiltering	Active ou désactive le filtrage d'URL via la base NETASQ dans le proxy. (Valeur par défaut : 1).
AntiSPAM	Active ou désactive le filtrage des spams via DNSBL dans le proxy. (Valeur par défaut : 1).

Matériel

Cette fenêtre présente les différentes données matérielles de votre équipement.

Haute disponibilité	Vérifie l'intégrité du cluster de HA (licences, configuration, synchronisation, membre actif).
Matériel	Présence ou non d'une clef USB sur le système (configuration sécurisée pour le module `Système\Maintenance`).
RAID	Etat du RAID (ensemble redondant de disques durs indépendant ou peu onéreux) et de ses disques, si l'option est disponible sur le matériel. ***A partir de la version 9.0.1,*** une alarme d'avertissement apparaîtra si un disque est défectueux ou manquant.

Propriétés

Cette fenêtre affiche les données essentielles de la configuration de votre firewall.

Propriétés

Numéro de série	Référence de votre firewall NETASQ.
Date	Date et heure en temps réel.
Partition de sauvegarde	Présence ou non d'une partition de sauvegarde sur votre système (cf Menu `Système\`module `Maintenance`\onglet `Configuration`).
Uptime	Temps depuis lequel le firewall tourne sans interruption.
Configuration LDAP	Etat de la connexion avec le LDAP.

Politique

Filtrage	Profil appliqué pour la politique de filtrage et NAT.
VPN	Etat du VPN sur votre réseau.

Active Update

Nom de l'objet	Nom du module listé.
Etat	Module à jour ou non.
Dernière mise à jour	Date et heure de la dernière mise à jour.

Services

Services	Liste des différents services disponibles sur l'équipement.
Uptime	Temps depuis lequel le service est actif sans interruption.
% CPU	Etat du service.

Interfaces

Nom de l'objet	Nom de l'interface in, out ou dmz.
Type	Il peut s'agir d'une interface physique (ethernet), VLAN, ou modem (dialup)
Adresse	Adresse IP et masque de sous-réseau de l'interface.
Débit entrant	Trafic entrant en Ko.
Débit sortant	Trafic sortant en Ko.

A partir de la version 9.0.1, les interfaces désactivées seront bien affichées sur le Tableau de Bord.

TRACES - SYSLOG

L'écran de configuration des traces se compose de 2 onglets :

- Stockage local
- Syslog

Onglet « Stockage local »

La configuration des traces permet d'allouer de l'espace disque pour chaque type de traces du firewall. Ce menu permet également la modification du comportement du firewall lors de l'enregistrement de ces traces.

Cet écran se divise en 2 parties :

- En haut : un menu présentant différentes options
- En bas : Un tableau

NOTE : Cet onglet est grisé si le firewall est un modèle sans disque dur. Dans ce cas, lors de l'ouverture du module, l'onglet `Syslog` s'affiche directement.

Si le quota d'espace disque est atteint

Vous avez la possibilité de choisir l'action à entreprendre lorsque le quota d'espace disque est atteint. Les différentes possibilités sont :

- **Effacer les traces les plus anciennes** : les traces les plus récentes effacent les traces les plus anciennes.
- **Interrompre l'écriture des traces** : les traces ne sont plus mémorisées sur le firewall.

Configuration de l'espace réservé pour les traces

Le firewall gère un certain nombre de fichiers de traces destinés à recueillir les événements détectés par les fonctions de journalisation. Les fichiers concernés par les événements de sécurité sont :

- **Alarmes** : événements liés à l'application des fonctions de prévention des intrusions (l_alarm),
- **Authentification** : événements liés à l'authentification des utilisateurs (l_auth),
- **Connexions réseaux :** événements liés aux connexions à travers et à destination du firewall (l_connection),
- **Politique de filtrage** : événements liés à l'application des fonctions de filtrage (l_filter),
- **Proxy FTP** : événements liés au trafic FTP (l_ftp),
- **Statistiques :** événements liés au monitoring temps réel (l_monitor),
- **Connexions applicatives (plugin)** : événements liés au traitement des plugins de l'ASQ (l_plugin),

- **Proxy POP3 :** événements liés à l'envoi des messages (l_pop3),
- **Applications et vulnérabilités (Seismo) :** événements liés à l'application de consultation des vulnérabilités sur le réseau NETASQ SEISMO (l_pvm),
- **Administration (Serverd) :** événements liés au serveur d'administration des firewalls : "serverd" (l_server),
- **Proxy SMTP :** événements liés au trafic SMTP (l_smtp),
- **Evénements systèmes** : c'est dans ce journal que sont enregistrés les événements liés directement au système : arrêt/démarrage du firewall, erreur système, etc. L'arrêt et démarrage des fonctions de journalisation correspondent à l'arrêt et au démarrage des « démons » qui génèrent les traces (l_system),
- **VPN IPSec** : événements liés à l'établissement des SA (l_vpn),
- **Proxy HTTP** : événements liés au trafic HTTP (l_web),
- **VPN SSL :** événements liés à l'établissement du VPN SSL (l_xvpn),

Les fichiers partagent un espace global de stockage avec d'autres fichiers de traces.
Pour chaque menu de traces (Alarmes, Authentification, Connexions réseaux, Politique de filtrage, Proxy FTP, Statistiques, Connexions applicatives (plugin), Proxy POP3, Applications et vulnérabilités (Seismo), Serveur, Proxy SMTP, Evénements systèmes, VPN IPSec, Proxy HTTP, VPN SSL), vous pouvez limiter la taille du fichier de traces en sélectionnant la taille du fichier en pourcentage de l'espace réservé pour les fichiers de logs.

Le tableau présente les colonnes suivantes :

Activé	Permet d'activer/désactiver le fichier de traces. Si vous décochez la ligne, le pourcentage est à 0. Dans ce cas, le type de log ne sera pas stocké sur le disque. En recochant la ligne, le pourcentage indiqué est à 1% par défaut.
Famille	Nom du fichier de traces.
Pourcentage	Taux d'occupation actuel en pourcentage. En cliquant dans une case, il est possible de modifier le pourcentage.
Quota d'espace disque	Proportion d'espace disque qu'occupe chaque fichier sur le disque qui varie selon le pourcentage spécifié.

En bas à droite du tableau est indiqué le total des pourcentages. Si le total est supérieur à 100%, dans ce cas, une ligne d'avertissement au bas de la grille est indiquée en rouge. (*Exemple : « Attention, répartition incorrecte : 113% de l'espace disponible est réservé)*. Les modifications sont toutefois autorisées.
En cliquant sur **Appliquer**, le message suivant s'affiche : « L'espace disque total réservé pour les traces dépasse la capacité pour ce modèle. Voulez-vous vraiment appliquer cette configuration ? ». Vous avez le choix entre forcer l'enregistrement ou annuler.



NOTE
Ces fichiers peuvent être copiés sur la solution NETASQ EVENT ANALYZER afin de construire des rapports ou d'effectuer leur archivage.

Onglet « Syslog »

L'onglet Syslog permet de configurer l'envoi des traces par Syslog.

Activer l'envoi des traces par syslog	Le firewall NETASQ vous permet d'envoyer automatiquement les traces vers un serveur dédié. Les traces sont envoyées au format WELF. Ce serveur peut être un serveur hébergeant la solution NETASQ EVENT ANALYZER ou bien un serveur SYSLOG quelconque. Lorsque le syslog est activé, le firewall envoie des paquets UDP (port 514 par défaut) contenant les lignes de log (une ligne par paquet).
Serveur(s) de destination	Indication de l'adresse IP ou de l'objet machine sur laquelle est installée la solution NETASQ EVENT ANALYZER ou un serveur SYSLOG.
Port	Indication du port de communication associé au serveur SYSLOG.

Famille de traces envoyées

Activé	Permet d'activer le fichier de traces.
Famille	Catégorie de fichier à envoyer (Alarme, Connexion, Web, Filtrage…).

Configuration avancée

Catégorie (facility)	Numéro ajouté au début d'une ligne de log. Il peut être utilisé pour différencier plusieurs appliances lorsqu'elles envoient leurs logs vers un même serveur Syslog.

Envoi des traces vers un serveur SYSLOG

1. Cocher la case Activer l'envoi des traces par syslog,
2. Indiquer le nom du serveur de destination,
3. Indiquer le port de communication associé au serveur de destination.

Les traces peuvent aussi être conservées sur le firewall (sauf modèles U30 et U70).

UTILISATEURS

Le service d'authentification des utilisateurs nécessite la création de comptes utilisateurs au niveau du firewall. Pour accéder aux fonctionnalités de ce module, vous devez avoir, au préalable, créé ou configuré votre base LDAP (voir document *Configuration de l'annuaire* ou module `Utilisateurs\Configuration de l'annuaire`).

Les comptes contiennent l'ensemble des informations relatives à ces utilisateurs :

- Identifiant de connexion
- Nom
- Prénom
- Mail (optionnel)
- Téléphone (optionnel)
- Description (optionnel)

L'écran des `Utilisateurs` se décompose en 2 parties :

- Un bandeau affichant les différentes options
- La liste des **CN** (ou utilisateurs) dans la colonne de gauche, accompagnés de leurs informations dans la colonne de droite.

Les actions possibles

La barre de recherche

Si vous recherchez un utilisateur ou un groupe d'utilisateurs en particulier, saisissez son nom.
Le champ de recherche vous permet de lister tous les utilisateurs et/ou groupes d'utilisateurs dont le nom, le prénom, et/ou le login correspondent aux mots clefs saisis.
Exemple :
Si vous saisissez la lettre « a » dans la barre de recherche, la liste en dessous fera apparaître tous les utilisateurs ou groupes d'utilisateurs possédant un « a » dans leur nom et/ou prénom.

Le filtre

Ce bouton permet de choisir le type de CN à afficher. Un menu déroulant vous propose les choix suivants :

Groupes et utilisateurs	Matérialisé par l'icône, cette option permet d'afficher dans la liste des CN à gauche, les utilisateurs et les groupes d'utilisateurs.
Utilisateurs	Matérialisé par l'icône, cette option permet d'afficher uniquement les utilisateurs dans la colonne de gauche.
Groupes	Matérialisé par l'icône, cette option permet d'afficher uniquement les groupes d'utilisateurs dans la colonne de gauche.

Créer un groupe

L'écran du module `Utilisateurs` vous propose, dans la colonne de droite, de renseigner les informations du groupe que vous souhaitez créer.

Nom	Donner un nom à votre groupe afin de l'identifier dans la liste des CN. **REMARQUE** Vous ne pourrez plus changer le nom de votre groupe une fois ce dernier créé.
Description	Vous pouvez décrire le groupe et modifier le contenu de sa description dès que vous le souhaitez. Remplir ce champ reste facultatif mais néanmoins recommandé.

CN

Filtrer (barre de recherche)	Vous pouvez saisir une chaîne de caractères afin de filtrer la liste des membres, ou vider ce champ pour afficher la liste complète.
Ajouter	Il est possible d'ajouter un utilisateur au groupe de 2 manières différentes : Lorsque vous cliquez sur le bouton **Ajouter**, une ligne vide vient se positionner en haut du tableau. Déroulez la liste des utilisateurs existants à l'aide de la flèche de droite et sélectionnez celui que vous désirez inclure au groupe. Vous pouvez également effectuer un 'glisser-déposer' en important un utilisateur depuis la liste des CN, dans la colonne de gauche.
Supprimer	Pour retirer un membre du groupe, sélectionnez-le et cliquez sur le bouton **Supprimer**. ***A partir de la version 9.0.1,*** lorsqu'un utilisateur est supprimé, la révocation de son certificat est proposée à l'administrateur..

Afin de valider la création de votre groupe et de ne perdre aucune modification apportée, cliquez sur **Appliquer**.

Créer un utilisateur

Pour créer un utilisateur, renseignez au moins son identifiant et son nom. Pour lui associer un certificat, vous devrez indiquer une adresse mail valide.

Id	Identifiant de connexion de l'utilisateur
Nom	Nom de l'utilisateur
Prénom	Prénom de l'utilisateur
Mail	Adresse e-mail de l'utilisateur. Celle-ci sera utile pour la création d'un certificat.
Téléphone	Numéro de téléphone de l'utilisateur.
Description	Description indicative à l'utilisateur.



REMARQUE

Les champs « Id », « Nom » et « Prénom » ne seront plus modifiables après leur création.

Afin de valider la création de votre utilisateur et de ne perdre aucune modification apportée, cliquez sur **Appliquer**.

Supprimer

Ce bouton permet de supprimer un utilisateur ou un groupe :

1 Sélectionnez l'utilisateur ou le groupe à supprimer.

2 Cliquez sur **Supprimer,** une fenêtre affichant le message « *Confirmez-vous l'effacement de l'utilisateur* <***nom de l'utilisateur***> » s'affiche. Cliquez sur **Oui**.

Vérifier l'utilisation

Matérialisé par l'icône , ce bouton vous renseigne sur les groupes dont vos utilisateurs font partie, ainsi que sur l'utilisation de l'utilisateur ou du groupe dans le reste de la configuration.
Exemple :
Le filtrage.

1 Sélectionnez l'utilisateur ou le groupe pour lequel vous souhaitez vérifier l'utilisation.

2 Cliquez sur le bouton **Vérifier l'utilisation**. L'arborescence des menus de gauche vous présente votre utilisateur/groupe (par son identifiant) au sein de l'onglet `User ans groups`, et affiche la liste des groupes dont celui-ci fait partie, ainsi que son utilisation dans la configuration du firewall.

La liste des utilisateurs (CN)

Lorsque vous souhaitez accéder aux données d'un utilisateur, sélectionnez-le dans la liste des CN de gauche, et les informations le concernant apparaissent dans la colonne de droite.

L'onglet « Compte »

Modifier le mot de passe	En cliquant sur cette option, vous pouvez créer le mot de passe d'authentification de l'utilisateur dans une fenêtre spécifique, affichant également le niveau de sécurité. **NOTE** Pour autoriser l'utilisateur à modifier son mot de passe lui-même, il faut vous rendre dans le menu `Utilisateurs`\module `Authentification`\onglet(s) `Interfaces internes` (ou `externes`)\`Mot de passe des utilisateurs` et cocher l'option **Les utilisateurs peuvent changer leur mot de passe**.
Id (non modifiable)	L'identifiant de connexion de l'utilisateur sélectionné.
Nom (non modifiable)	Le nom de l'utilisateur sélectionné.
Prénom (non modifiable)	Le prénom de l'utilisateur sélectionné.
Mail	Indique l'adresse e-mail de l'utilisateur sélectionné.
Téléphone	Le numéro de téléphone de l'utilisateur sélectionné.
Description	Description relative à l'utilisateur sélectionné.

L'onglet « Certificat »

Cet onglet vous permet de gérer le certificat x509 de l'utilisateur.
La PKI ne possédant pas d'Autorité de certification pas défaut, vous devez en créer une afin de gérer les certificats des utilisateurs : il faut vous rendre dans le menu `Objets réseaux`\onglet `Certificats et PKI\`bouton **Ajouter\Ajouter une autorité racine**.
Ce certificat peut servir dans deux cas : authentification via SSL et accès en VPN au firewall avec un client mobile IPSEC. Ce certificat peut aussi être utilisé par d'autres applications.

L'onglet « Membres des groupes »

Il permet d'inclure l'utilisateur dans un ou plusieurs groupes :
1 Cliquez sur le bouton **Ajouter**, une ligne vierge vient s'ajouter au tableau des groupes.
2 Sélectionnez la flèche à droite du champ, un menu déroulant vous propose une liste de groupes existants. Cliquez sur le groupe de votre choix, celui-ci vient s'ajouter à votre tableau.

Pour retirer un groupe, sélectionnez-le et cliquez sur le bouton **Supprimer**.

VPN IPSEC

Protocole standard, l'IPSec (IP Security) permet la création de tunnels VPN entre deux machines, entre une machine et un réseau, entre deux réseaux et tout type d'objet supportant le protocole.

Les services proposés par l'IPSec NETASQ offrent le contrôle d'accès, l'intégrité en mode non connecté, l'authentification de l'origine des données, la protection contre le rejeu, la confidentialité au niveau du chiffrement et sur le flux de trafic.

Vous pouvez par exemple, créer un tunnel entre deux firewalls ou entre le firewall et des clients nomades sur lesquels seraient installés des clients VPN.

L'écran du module VPN IPSec est composé de 4 onglets :

- `Politique de chiffrement – Tunnels` **:** cet onglet permet de créer vos tunnels IPSec entre deux firewalls (**Site à site – Gateway- Gateway**) ou entre un firewall multifonctions NETASQ et un utilisateur nomade (**Anonyme – Utilisateurs nomades**). 10 politiques de chiffrement vierges peuvent être configurées, activées et éditées. La politique anonyme permet aussi de configurer des tunnels avec un autre firewall, mais qui ne dis**p**ose pas d'une IP fixe. Il a alors la même contrainte qu'un nomade "classique": une IP non prévisible.
- `Correspondants` : vous pourrez ici créer de nouveaux correspondants (site distant ou correspondant anonyme nomade) en renseignant notamment leur **profil IKE**, leur méthode de négociation, ainsi que les paramètres spécifiques à chaque méthode de négociation.
- `Identification` : cet onglet permet de lister vos autorités de certification acceptées dans les tunnels utilisant les méthodes PKI, ainsi que les clés pré-partagées (PSK) de vos tunnels nomades dans deux tableaux.
- `Profils de chiffrement` : définissez ici vos profils de chiffrement IKE (phase 1) et IPsec (phase 2), ajoutez-en de nouveaux, établissez leur durée de vie maximum (en secondes). Vous pouvez également définir les propositions de négociation au niveau des algorithmes d'authentification et de chiffrement.

L'onglet « Politique de chiffrement – Tunnels »

La barre des profils	Le menu déroulant propose 10 profils IPSec numérotés de (1) à (10). Pour sélectionner un profil afin d'établir une configuration, cliquez sur la flèche à droite du champ.
Activer cette politique	Active immédiatement la politique IPSec sélectionnée : les paramètres enregistrés dans ce slot écrasent les paramètres en vigueur.
Editer	Cette fonction permet d'effectuer 3 actions sur les profils : • **Renommer** : en cliquant sur cette option, une fenêtre composée de deux champs à remplir s'affiche. Celle-ci propose de modifier le nom d'une part et d'ajouter un commentaire d'autre part. Une fois l'opération effectuée, cliquez sur « Mis à jour ». Il est également possible d' « annuler » la manipulation.

	Réinitialiser : Suppression de toutes les modifications apportées au profil **Copier vers** : Cette option permet de copier un profil vers un autre, toutes les informations du profil copié seront transmises au profil récepteur. Il portera également le même nom.
Dernière modification	Cette icône permet de connaître la date et l'heure de la dernière modification effectuée.
Désactiver la politique	Ce bouton permet de désactiver immédiatement la politique IPSec sélectionnée.

Site à site (Gateway-Gateway)

Cet onglet va permettre de créer un tunnel VPN entre deux éléments réseaux compatibles.

On appelle également ce type de procédé : *Tunnel VPN passerelle à passerelle* ou *tunnel Gateway to Gateway*.

Rechercher	La recherche s'effectuera sur le nom de l'objet et de ses différentes propriétés, sauf si vous avez spécifié dans les préférences de l'application de restreindre cette recherche aux noms d'objet.
Supprimer	Sélectionnez le tunnel VPN IPSec à retirer de la grille et cliquez sur ce bouton. **AVERTISSEMENT** Aucune fenêtre de confirmation de suppression ne s'afficher et votre règle sera directement retirée.
Monter	Placer la ligne sélectionnée avant celle du dessus.
Descendre	Placer la ligne sélectionnée après celle du dessous.

Ajouter

Afin de réaliser la configuration du tunnel, sélectionnez la politique VPN dans lequel vous désirez réaliser le tunnel. L'assistant de politique VPN IPSec vous aiguille alors dans la configuration.

Tunnel site à site

Vous allez ici définir chacune des extrémités de votre tunnel ainsi que le correspondant.

Choix du correspondant	Ceci est l'objet correspondant à l'adresse IP publique de l'extrémité du tunnel, soit, du correspondant VPN distant. La liste déroulante affiche par défaut « None ». Vous pouvez créer un correspondant via l'option suivante ou en choisir un dans la liste de ceux qui existent déjà.
Créer un correspondant	Définissez les paramètres de votre correspondant, plusieurs étapes sont nécessaires : 1 Sélection de la passerelle : ***Passerelle distante*** : choisissez l'objet correspondant à l'IP de l'extrémité du tunnel au sein de la liste déroulante. Vous pouvez également en ajouter à l'aide du bouton + . ***Nom*** : vous pouvez spécifier un nom pour votre passerelle ou conserver le nom

	d'origine du correspondant, qui sera précédé de la mention « Site_ » (« Site_<nom de l'objet> »). Cliquez sur **Suivant**. 2 Identification du correspondant : 2 choix sont possibles, l'identification par **Certificat** ou par **Clé pré partagée (PSK – *Pre-Shared Key*)**. Cochez l'option voulue. 1) Si vous optez pour le **Certificat**, vous devrez le sélectionner parmi ceux que vous avez créé préalablement au sein du module `Certificats et PKI`. 2) Si vous optez pour la **Clé pré partagée (PSK),** il vous faudra définir le secret que partageront les deux correspondants du tunnel VPN IPSec, sous forme d'un mot de passe à confirmer dans un second champ. Vous pouvez **Saisir la clé en caractères ASCII** (chaque caractère d'un texte en ASCII est stocké dans un octet dont le 8[e] bit est 0.) en cochant la case correspondante. Décochez la case pour afficher la clé en caractères hexadécimaux (dont le principe repose sur 16 signes : les lettres de A à F et les chiffres de 0 à 9). Cliquez sur **Suivant.** 3 Terminer la création du correspondant : L'écran vous présente une fenêtre récapitulative de la configuration effectuée, les **Paramètres du site distant** et la **Clé pré partagée**. Vous pouvez également ajouter un correspondant de secours en cliquant sur le lien joint. Vous devrez renseigner la passerelle distante. Cliquez sur **Terminer**.
Réseau local	Machine, groupes de machines, plage d'adresses, réseau ou groupe de réseaux qui vont être accessibles via le tunnel VPN IPSec.
Réseau distant	Machine, groupes de machines, plage d'adresses, réseau ou groupe de réseaux faisant référence au correspondant VPN en vis-à-vis de votre firewall et inversement. Les deux correspondants doivent pouvoir négocier le trafic d'un côté et de l'autre.

Configuration en étoile

Ce procédé consiste à diriger plusieurs tunnels VPN vers un même point. Il permet, par exemple, de relier des agences à un site central.

Réseau local	Choisissez votre machine, groupes de machines, plage d'adresses, réseau ou groupe de réseaux qui sera accessible via le tunnel VPN IPSec, au sein de la liste déroulante d'objets.
Sites distants	Définissez les paramètres de vos sites distants : choisissez votre correspondant parmi la liste de ceux déjà créés ou cliquez sur l'icône », pour en créer un nouveau, et sélectionnez les réseaux distants parmi les objets de la liste déroulante. Vous pouvez en **Ajouter** ou en **Supprimer** en cliquant sur les boutons prévus à cet effet.
Considérer les réseaux distants comme des réseaux internes	Par défaut, l'interface IPSec est considérée comme externe. En cochant cette case, l'interface passe en mode « protégée ».

Cliquez sur **Terminer**.

Séparateur – regroupement de règles

Cette option permet d'insérer un séparateur au dessus de la ligne sélectionnée. Cela peut permettre à l'administrateur de hiérarchiser ses tunnels comme il le souhaite.

La grille

Ligne	Cette colonne indique le numéro de la ligne (1,2,3…) traitée par ordre d'apparition à l'écran.
Etat	Cette colonne affiche l'état **On**/ **Off** du tunnel. Lorsque vous en créez un, celui-ci s'active par défaut. Cliquez une fois dessus pour le désactiver.
Réseau local	Choisissez votre machine, groupes de machines, plage d'adresses, réseau ou groupe de réseaux qui sera accessible via le tunnel VPN IPSec, au sein de la liste déroulante d'objets.
Correspondant	Configuration de correspondant, visible au sein de l'onglet du même nom dans le module VPN IPSec.
Réseau distant	Choisissez parmi la liste déroulant d'objets, votre machine, groupes de machines, plage d'adresses, réseau ou groupe de réseaux faisant référence au correspondant VPN en vis-à-vis de votre firewall ; par exemple l'adresse IP publique connue de votre correspondant.
Profil de chiffrement	Cette option permet de choisir le modèle de protection associé à votre politique VPN, parmi les 3 profils préconfigurés : **StrongEncryption, GoodEncryption et FastEncryption** Il est possible de créer ou de modifier d'autres profils au sein de l'onglet « `Profils de chiffrement` ».
Commentaire	Description associée à la politique VPN.

Anonyme – Utilisateurs nomades

Le VPN IPSec comporte deux extrémités : l'extrémité de tunnel, et l'extrémité de trafic. Pour les anonymes ou utilisateurs nomades, l'IP d'extrémité de tunnel n'est pas connue à l'avance.
L'IP d'extrémité de trafic, quant à elle, peut être soit choisie par le correspondant (cas « classique »), ou distribuée par la passerelle (« Mode Config »).

Nom de la configuration nomade

Par défaut, la liste déroulante affichera le message « pas de correspondant trouvé », pour y remédier, la procédure à suivre est la suivante :

1 Cliquez sur le bouton « **Ajouter** » une « **Nouvelle Politique** » VPN, puis sur « **Créer un correspondant nomade** » via l'assistant de politique VPN IPSec nomade.

2 Donnez un nom à votre configuration nomade, et cliquez sur **Suivant**.

3 Choisissez la méthode d'authentification du correspondant.

Certificat	Si vous optez pour cette méthode d'authentification, vous devrez ensuite choisir votre **Certificat** (serveur) à présenter au correspondant, parmi la liste de ceux que vous avez créé au préalable (`Module Certificats et PKI`). Vous pourrez également fournir l'« **Autorité de confiance** » (CA) ayant signé le

	certificat de votre correspondant.
Hybride	Si vous optez pour la méthode hybride, vous devrez également fournir un « **Certificat** » (serveur) à présenter au correspondant et éventuellement, sa CA. Elle est utilisée avec IKE et présente une asymétrie entre les différentes méthodes d’authentification, qui combinent la méthode par certificat et par PSK.
Certificat et XAuth (Iphone)	Cette option permet aux utilisateurs mobiles de se connecter sur la passerelle VPN de votre entreprise via leur téléphone portable, à l’aide d’un un certificat. **NOTE** C’est le seul mode compatible avec l’Iphone.
Clé pré partagée (PSK)	Si vous optez pour cette méthode d’authentification, vous devrez éditez votre clé dans un tableau, en fournissant son ID, et sa valeur à confirmer. Pour cela, cliquez sur **Ajouter**. L’ID peut-être au format IP (X.Y.Z.W), FQDN (monserveur.domain.com), e-mail (toto.dupont@domain.com). Il occupera ensuite la colonne « Identité » du tableau et la PSK occupera une colonne du même nom avec sa valeur affichée en hexadécimal.

Cliquez sur **Suivant**.

4 Vérifiez l’écran de résumé de votre configuration nomade et cliquez sur **Terminer**.

5 Renseignez ensuite la ressource locale, ou « **réseau local** » vers lequel sera dirigé votre utilisateur nomade.

Vous pouvez également effectuer d’autres actions :

Rechercher	La recherche s’effectuera sur le nom de l’objet et de ses différentes propriétés, sauf si vous avez spécifié dans les préférences de l’application de restreindre cette recherche aux noms d’objet.
Supprimer	Sélectionnez le tunnel VPN IPsec à retirer de la grille et cliquez sur ce bouton. **AVERTISSEMENT** Aucune fenêtre de confirmation de suppression ne s’afficher et votre règle sera directement retirée.
Monter	Placer la ligne sélectionnée avant celle du dessus.
Descendre	Placer la ligne sélectionnée après celle du dessous.

La grille

Ligne	Cette colonne indique le numéro de la ligne (1,2,3…) traitée par ordre d’apparition à l’écran
Etat	Cette colonne affiche l’état **On**/ **Off** du tunnel. Lorsque vous en créez un, celui-ci s’active par défaut. Cliquez une fois dessus pour le désactiver.
Réseau local	Choisissez votre machine, groupes de machines, plage d’adresses, réseau ou groupe de réseaux qui sera accessible via le tunnel VPN IPSec, au sein de la liste déroulante d’objets.
Correspondant	Configuration de correspondant, visible au sein de l’onglet du même nom dans le module VPN IPSec.
Réseau distant	Choisissez parmi la liste déroulant d’objets, votre machine, groupes de machines, plage d’adresses, réseau ou groupe de réseaux faisant référence au

	correspondant VPN en vis-à-vis de votre firewall. **NOTE** Lorsque vous créez une nouvelle politique VPN IPSec nomade via l'assistant, il vous est demandé de fournir le réseau local, et non le réseau distant, puisque l'adresse IP n'est pas connue. L'objet « Any » sera donc choisi par défaut.
Profil de chiffrement	Cette option permet de choisir le modèle de protection associé à votre politique VPN, parmi les 3 profils préconfigurés : **StrongEncryption, GoodEncryption** et **FastEncryption**. Il est également de créer et de modifier d'autres profils au sein de l'onglet « `Profils de chiffrement` ».
Mode config	Cette colonne rend possible l'activation du « Mode config », désactivé par défaut. Celui-ci permet de distribuer l'IP d'extrémité de trafic au correspondant. **NOTES** 1) Si vous choisissez d'activer ce mode, vous devrez sélectionner un objet autre qu'« Any » en tant que réseau distant. 2) Avec le mode config, une seule politique peut être appliquée par profil.
Commentaire	Description associée à la politique VPN.



REMARQUE

Vous ne pourrez utiliser et créer qu'un seul nomade (« roadwarrior ») par profil IPSec.
Les correspondants sont applicables à tous les profils.

L'onglet « Correspondants»

Cet onglet est divisé en deux écrans :

- A gauche : la liste des correspondants VPN IPSec et VPN IPSec nomades.
- A droite : Les informations du correspondant sélectionné.

La liste des correspondants

Chercher dans les correspondants	Ce champ permet d'effectuer une recherche sur le nom de l'objet et ses différentes propriétés, par occurrence, lettre ou mot.
Filtrer	3 choix sont possibles : Vous pouvez afficher dans la liste « **Tous les correspondants** », passerelles et nomades confondus. Vous pouvez également ne laisser apparaître que les « **Passerelles** » ou uniquement les « **Correspondants mobiles** » (nomades).
Ajouter	Il est possible d'ajouter des correspondants à cet endroit précis. Pour cela, choisissez parmi la liste déroulante le type de correspondant à créer : un « **Nouveau site distant** » ou un « **Nouveau correspondant nomade** ». Vous pouvez aussi « **Copier depuis la sélection** » un correspondant, celui-ci sera dupliqué. Pour cela, positionnez-vous sur le correspondant à copier et entrez son nouveau nom dans la fenêtre affichée.
Supprimer	Sélectionnez le correspondant à retirer de la liste et cliquez sur **Supprimer**.
Nom	Nom donné au correspondant lors de sa création.

Les informations des correspondants

Correspondant (de type « passerelle »)

Commentaire	Description associée au correspondant local.
Passerelle distante	Objet sélectionné pour la passerelle distante lors de la création du correspondant via l'assistant.
Configuration de secours	Ce champ précise si vous avez défini une configuration de secours lors de la création du correspondant, il affichera « None » par défaut si vous n'en avez créé aucune. Vous pouvez toutefois en définir une en la sélectionnant dans la liste déroulante contenant vos autres correspondants distants.
Profil IKE	Cette option permet de choisir le modèle de protection associé à votre politique VPN, parmi les 3 profils préconfigurés : **StrongEncryption**, **GoodEncryption**, **FastEncryption**. Il est possible de créer ou de modifier d'autres profils au sein de l'onglet « `Profils de chiffrement` ».

Identification

Méthode d'authentification	Ce champ affichera la méthode d'authentification choisie lors de la création de votre correspondant via l'assistant. Vous pouvez modifier votre choix en sélectionnant une autre méthode d'authentification présente dans la liste déroulante.  **NOTE** Pour un correspondant de type « passerelle », vous avez le choix entre **Certificat** ou **Clé pré partagée (PSK)**.
Certificat	Si vous avez choisi la méthode d'authentification par certificat, ce champ affichera votre certificat. Si vous avez opté pour la clé pré partagée, ce champ sera grisé.
Local ID (Optionnel)	Ce champ représente une extrémité du tunnel VPN IPSec, partageant le « secret » ou la PSK avec le « Peer ID », autre extrémité. Le « Local ID » vous représente.
Peer ID	Ce champ représente une extrémité du tunnel VPN IPSec, partageant le « secret » ou la PSK avec le « Local ID », autre extrémité. Le « Peer ID » représente votre correspondant.
Clé pré partagée (ASCII)	Dans ce champ apparaît votre PSK sous le format que vous avez choisi précédemment lors de la création du correspondant via l'assistant : caractères ASCII ou hexadécimaux (case à cocher au bas du champ si vous souhaitez en changer).
Confirmer	Confirmation de votre clé pré partagée (PSK).

Configuration avancée

Mode de négociation	En IPSec, 2 modes de négociation sont possibles : le mode principal (ou « main » mode) et le mode agressif. Ils influent notamment sur la « phase 1 » du protocole IKE (phase « d'authentification »). **Mode principal**: Dans ce mode, la phase 1 se déroule en 6 échanges. La machine distante ne peut être identifiée que par son adresse IP avec une

	authentification en clés pré-partagée. En mode PKI, l'identifiant est dans le certificat. Le mode principal assure l'anonymat. **Mode agressif** : dans ce mode, la phase 1 se déroule en 3 échanges entre le firewall et la machine distante. La machine distante peut être identifiée avec une adresse IP, FQDN ou une adresse mail mais pas avec un certificat par clé pré-partagée. Le mode agressif n'assure pas l'anonymat.  **AVERTISSEMENT** L'utilisation du mode agressif + les clés pré-partagées (notamment pour les tunnels VPN à destination de nomades) peut se révéler moins sécuritaire que les autres modes du protocole IPsec. Ainsi NETASQ recommande l'utilisation du mode principal et en particulier du mode principal + certificats pour les tunnels à destination de nomades. En effet la PKI interne du firewall peut tout à fait fournir les certificats nécessaires à une telle utilisation.
Mode de secours	Le mode de secours est le mode de bascule pour le failover IPSec, si un serveur tombe, un autre prend le relai, de manière transparente. Deux choix sont possibles : Le mode « **temporaire** » : le correspondant principal est joint dès que possible. Le mode « **permanent** » : si le correspondant n'est pas joignable, vous basculerez sur un autre correspondant.  **NOTE** Ce champ n'est éditable qu'en mode expert (CLI).
Passerelle locale	Objet sélectionné pour la passerelle locale. Ce champ est en « Any » par défaut.
Ne pas initier le tunnel (Responder-only) :	Si vous cochez cette option, le serveur IPSec sera mis en attente. Il ne prendra pas l'initiative de négociation du tunnel. Cette option est utilisée dans le cas où le correspondant est un mobile.
DPD	Ce champ permet de configurer la fonctionnalité VPN dite de DPD (*Dead Peer Detection*). Celui-ci permet de vérifier qu'un correspondant est toujours opérationnel. Quand le DPD est actif sur un correspondant, celui-ci envoie régulièrement des paquets ou messages à l'autre correspondant, auxquels ce dernier répond pour dire qu'il est toujours là. Ces échanges sont sécurisés via les SAs (*Security Association*) ISAKMP (*Internet Security Association and Key Management Protocol*). Si on détecte qu'un correspondant ne répond plus, les SAs négociées sont détruites.  **AVERTISSEMENT** Cette fonctionnalité apporte une stabilité au service VPN sur les firewalls NETASQ, à la condition que le DPD soit correctement configuré. Pour configurer l'option de **DPD**, quatre choix sont disponibles : **Inactif** : les requêtes DPD provenant du correspondant sont ignorées. **Passif** : les requêtes DPD émises par le correspondant obtiennent une réponse du firewall. Par contre, le firewall n'en n'envoie pas. **Bas** : la fréquence d'envoi des paquets DPD est faible, et le nombre d'échecs tolérés est élevé. **Haut** : la fréquence d'envoi des paquets DPD est élevée et le nombre d'échecs est relativement bas



NOTE

Pour chaque champ comportant la mention « Passerelle » et l'icône, vous pourrez ajouter un objet à la base existante en précisant son nom, sa résolution DNS, son adresse IP et en cliquant ensuite sur **Appliquer**.

A partir de la version 9.0.1, le mode de négociation (principal ou agressif), lorsqu'il a été forcé, est conservé quand on modifie la configuration d'un correspondant IPSec.

Correspondant (de type nomade/ « correspondant mobile »)

Commentaire	Description associée au correspondant distant.
Passerelle distante	Ce champ est grisé pour les correspondants de type nomade.
Configuration de secours	Ce champ est grisé pour les correspondants de type nomade.
Profil IKE	Cette option permet de choisir le modèle de protection associé à votre politique VPN, parmi les 3 profils préconfigurés: **StrongEncryption**, **GoodEncryption**, et **FastEncryption**. Il est possible de créer ou de modifier d'autres profils au sein de l'onglet « `Profils de chiffrement` ».

Identification

Méthode d'authentification	Ce champ affichera la méthode d'authentification choisie lors de la création de votre correspondant via l'assistant. Vous pouvez modifier votre choix en sélectionnant une autre méthode d'authentification présente dans la liste déroulante. **NOTE** Pour un correspondant de type « nomade », vous avez le choix entre **Certificat**, **Clé pré partagée (PSK)**, **Hybride, Certificat et Xauth (Iphone).**
Certificat	Si vous avez choisi la méthode d'authentification par **Certificat**, **Hybride** ou **Certificat** et **XAuth**, ce champ affichera votre certificat ou vous proposera de le sélectionner au sein de la liste déroulante. Si vous avez opté pour la clé pré partagée, ce champ sera grisé.
Local ID (Optionnel)	Ce champ représente une extrémité du tunnel VPN IPSec, partageant le « secret » ou la PSK avec le « Peer ID », autre extrémité. Le « Local ID » vous représente. **NOTE** Ce champ n'est accessible que si vous avez choisi la méthode d'authentification par **Clé pré partagée**.
Cliquer ici pour éditer la liste des PSK	En cliquant sur ce lien, vous basculerez dans l'onglet « **Identification** » du module VPN IPSec. Vous pourrez y ajouter vos **Autorités de certification acceptées** ainsi que vos **Tunnels nomades : clés pré partagées**.

Configuration avancée

Mode de négociation	En IPSec, 2 modes de négociation sont possibles : le mode principal (ou « main » mode) et le mode agressif. Ils influent notamment sur la « phase 1 » du protocole IKE (phase « d'authentification »). **Mode principal** : Dans ce mode, la phase 1 se déroule en 6 échanges. La machine distante ne peut être identifiée que par son adresse IP avec une authentification en clé pré-partagée. En mode PKI, l'identifiant est dans le certificat. Le mode principal assure l'anonymat. **Mode agressif** : dans ce mode, la phase 1 se déroule en 3 échanges entre le firewall et la machine distante. La machine distante peut être identifiée avec une adresse IP, FQDN ou une adresse mail mais pas avec un certificat par clé pré-partagée. Le mode agressif n'assure pas l'anonymat.  **NOTE** NETASQ préconise l'utilisation des méthodes d'authentification par certificat, hybride ou XAuth avec le mode principal. Si le client veut utiliser la PSK, il doit se positionner en mode agressif.  **AVERTISSEMENT** L'utilisation du mode agressif + les clés pré-partagées (notamment pour les tunnels VPN à destination de nomades) peut se révéler moins sécuritaire que les autres modes du protocole IPSec. Ainsi NETASQ recommande l'utilisation du mode principal et en particulier du mode principal + certificats pour les tunnels à destination de nomades. En effet la PKI interne du firewall peut tout à fait fournir les certificats nécessaires à une telle utilisation.
Mode de secours	Le mode de secours est le mode de bascule pour le failover IPSec, si un serveur tombe, un autre prend le relai, de manière transparente. Néanmoins, ici, le champ est grisé car la configuration de secours n'est pas applicable pour une configuration nomade.  **NOTE** Ce champ n'est éditable qu'en mode expert (CLI).
Passerelle locale	Objet sélectionné pour la passerelle locale. Ce champ est en « Any » par défaut.
Ne pas initier le tunnel (Responder-only) :	Si vous cochez cette option le serveur IPSec sera mis en attente. Il ne prendra pas l'initiative de négociation du tunnel. Cette option est utilisée dans le cas où le correspondant est un mobile.
DPD	Ce champ permet de configurer la fonctionnalité VPN dite de DPD (*Dead Peer Detection*). Celui-ci permet de vérifier qu'un correspondant est toujours opérationnel. Quand le DPD est actif sur un correspondant, celui-ci envoie régulièrement des paquets ou messages à l'autre correspondant, auxquels ce dernier répond pour dire qu'il est toujours là. Ces échanges sont sécurisés via les SA (*Security Association*) ISAKMP (*Internet Security Association and Key Management Protocol*). Si on détecte qu'un correspondant ne répond plus, les SA négociées avec celui-ci sont détruites.

AVERTISSEMENT
Cette fonctionnalité apporte une stabilité au service VPN sur les firewalls NETASQ, à la condition que le DPD soit correctement configuré.

Pour configurer l'option de **DPD**, quatre choix sont disponibles :

Inactif : les requêtes DPD provenant du correspondant sont ignorées.

Passif : les requêtes DPD émises par le correspondant obtiennent une réponse du firewall. Par contre, le firewall n'en n'envoie pas.

Bas : la fréquence d'envoi des paquets DPD est faible, et le nombre d'échecs tolérés est élevé.

Haut : la fréquence d'envoi des paquets DPD est élevée et le nombre d'échecs est relativement bas.

L'onglet « Identification»

Autorités de certification acceptées

Ce tableau va permettre de lister les autorités pour identifier vos correspondants au sein du module VPN IPSec.

Ajouter	Lorsque vous cliquez sur ce bouton, une fenêtre regroupant les CA et sous CA que vous avez créé au préalable apparaît. Sélectionnez les autorités qui permettront de vérifier les identités de vos correspondants, en cliquant sur **Select**. La CA ou sous CA choisie vient s'ajouter au tableau.
Supprimer	Sélectionnez la CA à retirer de la liste et cliquez sur **Supprimer**.

CA

En dessous de ce champ figurent les autorités de certification ajoutées et acceptées.

Tunnels nomades : clés pré partagées

Si vous avez préalablement créé un correspondant nomade ayant pour méthode d'authentification la **Clé pré partagée (PSK)**, ce tableau sera déjà pré-rempli.
Vous aviez dû éditer une clé en lui définissant un ID et une valeur (en caractères hexadécimaux ou ASCII).

Rechercher	Bien que le tableau affiche toutes vos clés pré partagées de tunnels nomades par défaut, vous pouvez effectuez une recherche par occurrence, lettre ou mot, de manière à ce que seules les clés souhaitées s'affichent à l'écran.
Ajouter	En cliquant sur ce bouton, une fenêtre d'édition de clé s'affichera : vous devrez lui

	fournir un ID, une valeur, et confirmer cette dernière. Vous pourrez choisir d'éditer en caractères hexadécimaux ou ASCII.
Supprimer	Sélectionnez la clé à retirer de la liste et cliquez sur **Supprimer**.

Identité

Cette colonne affiche les ID de vos clés pré partagées, qui peuvent être représentés par un nom de domaine (FQDN), une adresse e-mail (USER_FQDN) ou une adresse IP.

Clé

Cette colonne affiche les valeurs de vos clés pré partagées en caractères hexadécimaux.



REMARQUES

La création de clés pré-partagées est illimitée.

La suppression d'une clé pré-partagée appartenant à un tunnel VPN IPSec entraîne le dysfonctionnement de ce tunnel.

L'onglet « Profils de Chiffrement »

Profils de chiffrement par défaut

Le déploiement et l'utilisation massive d'IPSec exige un protocole de gestion des SAs standard sur Internet, extensible et automatisé. Par défaut, le protocole de gestion automatisée des clefs choisi pour IPSec est IKE.
IKE est organisé autour de 2 phases de négociation :

Profil de chiffrement IKE (phase 1)

La phase 1 du protocole IKE vise à établir un canal de communication chiffré et authentifié entre les deux correspondants VPN. Ce "canal" est appelé SA ISAKMP (différent de la SA IPSec). Deux modes de négociations sont possibles : le mode principal et le mode agressif.

La liste déroulante permet de choisir le modèle de protection associé à votre politique VPN, parmi les 3 profils préconfigurés : **StrongEncryption, GoodEncryption,** et **FastEncryption**. Il est également possible d'en créer d'autres.

Profil de chiffrement IPsec (phase 2)

La phase 2 du protocole IKE négocie de manière sécurisée (au moyen du canal de communication SA
ISAKMP négocié dans la première phase) les paramètres des futures SA IPSec (une entrante et une sortante).

La liste déroulante permet de choisir le modèle de protection associé à votre politique VPN, parmi les 3 profils préconfigurés : **StrongEncryption, GoodEncryption,** et **FastEncryption**. Il est également possible d'en créer d'autres.

Tableau des profils

Ce tableau propose une série de profils de chiffrement prédéfinis, de phases 1 ou 2. Pour chaque profil sélectionné, vous verrez apparaître ses caractéristiques à droite de l'écran (champs « **Général** », « **Propositions d'authentification** » et « **Propositions de chiffrement** »).

Ajouter	En cliquant sur ce bouton, vous pourrez choisir d'ajouter un **Profil de phase 1** (IKE) ou **Profil de phase 2 (IPSec)**, qui sera affiché dans la colonne « Type ». Vous pourrez lui donner le « Nom » que vous souhaitez. Il est également possible de copier un profil et ses caractéristiques : pour cela, sélectionnez le profil voulu et cliquez sur l'option **Copier la sélection**, puis donnez lui un nom.
Supprimer	Sélectionnez le profil de chiffrement à retirer de la liste et cliquez sur **Supprimer**.

Général

Commentaire	Description associé à votre profil de chiffrement.
Diffie Hellman/Perfect Forward Secrecy (PFS)	Ce champ représente deux types d'échange de clé: si vous avez sélectionné un profil de chiffrement type **IKE**, c'est l'option **Diffie-Hellman** qui apparaîtra. **Diffie-Hellman** permet à 2 correspondants de générer chacun de leur coté un secret commun, sans transmission d'infos sensibles sur le réseau. En revanche, si vous optez pour un profil **IPSec**, le **PFS** vous sera proposé. Le **Perfect Forward Secrecy** permet de garantir qu'il n'y a aucun lien entre les différentes clés de chaque session. Les clés sont recalculées par l'algorithme de Diffie-Hellman sélectionné. Plus le chiffre est élevé, plus la sécurité est importante. Que vous choisissiez l'un ou l'autre, une liste déroulante vous propose de définir un nombre de bits qui permet de renforcer la sécurité lors de la transmission du secret commun ou mot de passe d'un correspondant à l'autre. Plusieurs choix (en octets) sont possibles : **768, 1024, 1536, 2048, 3072** et **4096**. **REMARQUE** Plus la taille du mot de passe (ou « clé ») est grande, plus le niveau de sécurité est élevé, mais consomme aussi davantage de ressources.
Durée de vie maximum (en secondes)	Période de temps au bout de laquelle les clés sont renégociées. La durée de vie par défaut pour un profil de type **IKE** est 21600 secondes, et 3600 secondes pour un profil de type **IPSec**.

Propositions d'authentification

Cette grille vous propose de modifier ou d'ajouter des algorithmes d'authentification à la liste pré établie du profil sélectionné.

Ajouter	L'algorithme d'authentification apparaissant par défaut en cliquant sur ce bouton est **hmac_sha1,** d'une « Force **»** de 160 bits et en priorité « 1 ». Cliquez sur la flèche à droite de la colonne « Algorithme » si vous souhaitez le modifier.

	Chaque fois que vous ajoutez une ligne au tableau, celle-ci passe en priorité suivante.
Supprimer	Sélectionnez la ligne à retirer de la liste et cliquez sur **Supprimer**.
Algorithme	6 choix vous sont proposés : **sha1, md5, sha256, sha384, sha512** ou **non_auth**.
Force	Nombre de bits définis pour l'algorithme sélectionné.

Propositions de chiffrement

Cette grille vous propose de modifier ou d'ajouter des algorithmes de chiffrement à la liste pré établie du profil sélectionné.

Ajouter	L'algorithme de chiffrement apparaissant par défaut en cliquant sur ce bouton est **des,** d'une « Force **»** de 64 bits. Cliquez sur la flèche à droite de la colonne « Algorithme » si vous souhaitez le modifier. Chaque fois que vous ajouter une ligne au tableau, celle-ci passe en priorité suivante.
Supprimer	Sélectionnez la ligne à retirer de la liste et cliquez sur **Supprimer**.
Algorithme	5 choix vous sont proposés : **des**, **3des**, **blowfish, cast128** et **aes**.
Force	Nombre de bits définis pour l'algorithme sélectionné.



Ces deux grilles ne s'affichent que si vous avez sélectionné le type de profil **IPSec**.
Pour un profil de type **IKE**, seule une grille « **Propositions** » s'affichera, divisée en deux colonnes : « Authentification » et « Chiffrement », avec leurs algorithmes respectifs.
Vous pourrez en **Ajouter** ou en **Supprimer**, en modifiant l'ordre de priorité à l'aide des boutons **Monter** et **Descendre**.

Cliquez sur **Appliquer** une fois votre configuration effectuée.

VPN SSL

Le VPN SSL NETASQ permet à vos utilisateurs nomades ou non de se connecter sur les ressources de votre société de façon sécurisée.

L'écran de configuration du VPN SSL se compose de 4 onglets :

- **`Général`** : Permet l'activation du module, le choix du type d'accès ainsi que la configuration avancée.
- **`Serveurs web`** : Le VPN SSL NETASQ permet de sécuriser les accès à vos serveurs HTTP (Intranet, webmail,…) tout en évitant de devoir gérer de multiples serveurs https. De plus, pour l'accès aux utilisateurs nomades, il permet de masquer les informations sur votre réseau interne, la seule adresse IP visible étant celle de votre firewall.

  Le VPN SSL NETASQ réécrit de façon automatique les liens HTTP trouvés dans les pages Web consultées par vos utilisateurs. Cela permet de naviguer entre vos différents serveurs, si ces derniers sont configurés, ou d'interdire l'accès à certains serveurs. Lorsqu'un lien web dans une page pointe sur un serveur non configuré, le lien est redirigé vers la page de démarrage du VPN SSL NETASQ.
- **`Serveurs applicatifs`** : Cette section rassemble les serveurs configurés pour les accès aux ressources autres que le type Web (telnet, mail)…

  Le VPN SSL NETASQ permet de sécuriser tout protocole basé sur une connexion TCP unique (POP3, SMTP, telnet, accès distant, ...). Dans le cadre de protocoles autres que l'HTTP, le client permettant la connexion sécurisée est une applet JAVA. Cette dernière ouvre un tunnel chiffré. Tous les paquets échangés entre le poste client et le firewall sont chiffrés.

  Le VPN SSL NETASQ n'impose pas d'installation de clients sur les postes de vos utilisateurs, et supporte nativement les OS disposant de JAVA (Windows, Linux, MAC OS-X,…).

  Il vous suffit de configurer les serveurs auxquels vous désirez donner l'accès à vos utilisateurs. Ces serveurs seront dynamiquement ajoutés à la liste des serveurs autorisés lors du prochain chargement de l'applet JAVA effectué par vos utilisateurs.

  L'applet JAVA ouvre des ports en écoute sur le poste client. C'est sur ces derniers que devront se connecter les outils clients afin de passer par le tunnel sécurisé établi entre l'applet et le firewall. Il est nécessaire de s'assurer que le port choisi est accessible à l'utilisateur (problème de droit) et qu'il ne peut pas entrer en conflit avec un port utilisé par un autre programme. Ces serveurs seront dynamiquement ajoutés. Cela peut être utilisé afin d'effectuer des contrôles et/ou authentifications transparentes sur la provenance des requêtes.
- **`Profils utilisateurs`** : Si vous souhaitez restreindre l'accès aux serveurs définis dans la configuration du VPN SSL, vous devez définir des profils contenant la liste des serveurs autorisés, puis de les attribuer aux utilisateurs.

L'onglet « Général »

Activer le VPN SSL : Permet d'activer le VPN SSL et de choisir entre les trois options proposées dans le tableau ci-dessous.

Uniquement l'accès aux serveurs web	Utilisation du module de VPN SSL pour l'accès aux ressources de type Web. Active l'onglet `Serveurs web`.

Uniquement l'accès aux serveurs applicatifs	Utilisation du module de VPN SSL pour l'accès aux ressources sur une connexion de type TCP. Active l'onglet `Serveurs applicatifs`.
L'accès aux serveurs web et applicatifs	Utilisation du module VPN SSL pour l'accès aux ressources de type Web et de type TCP. Active les deux onglets `Serveurs web` et `Serveurs applicatifs`.

Configuration avancée

Authentifier l'utilisateur à chaque requête (authentification par certificat ssl uniquement)	Si l'option **Authentifier l'utilisateur à chaque requête (authentification par certificat ssl uniquement)** est cochée, chaque requête transitant par le module de VPN SSL des firewalls NETASQ nécessite une authentification par certificat de l'utilisateur émetteur de la requête.

Accès aux serveurs via le VPN SSL

Préfixe du répertoire racine de l'URL	La technologie VPN SSL NETASQ permet de masquer l'adresse réelle des serveurs vers lesquels les utilisateurs sont redirigés en réécrivant l'ensemble des URL contenues dans les pages HTTP rencontrées. Ces URL sont remplacées par un préfixe suivi de 4 chiffres. Ce champ permet de définir le préfixe qui sera utilisé.
En-tête HTTP pour l'identifiant utilisateur	La valeur de ce champ sera envoyée, accompagnée de l'identifiant de l'utilisateur, au serveur Web dans l'entête HTTP des requêtes émises. Cette valeur peut être utilisée afin d'effectuer des contrôles et/ou authentification transparentes sur la provenance des requêtes. Dans le cas où le serveur vers lequel les flux HTTP sont redirigés demande une authentification, il est possible de spécifier un login dans l'entête du paquet HTTP. Ce login pourrait servir par exemple à indiquer que ces flux arrivant au serveur proviennent du firewall et peuvent être accepté par le serveur sans authentification.

Configuration du poste client

Commande exécutée au démarrage	Exécutée au lancement de l'applet, cette commande permet à l'administrateur de définir des actions préalables à l'affichage de l'applet. Par exemple, cette commande pourrait lancer un script présent sur un serveur et qui modifierait les paramètres du compte de messagerie de l'utilisateur de telle façon que lorsque l'applet est lancée, les flux SMTP ou POP soit automatiquement redirigé, sans intervention de l'utilisateur.
Commande exécutée à l'arrêt	Exécutée à la fermeture de l'applet, cette commande permet à l'administrateur de définir des actions préalables à la fermeture de l'applet. Par exemple, cette commande pourrait lancer un script présent sur un serveur et qui modifierait les paramètres du compte de messagerie de l'utilisateur de telle façon que lorsque l'applet est fermée, les flux SMTP ou POP ne sont plus automatiquement redirigé et encore une fois sans intervention de l'utilisateur.

L'onglet « Serveurs web »

Cette section rassemble les serveurs configurés pour les accès aux ressources de type Web.

Le nombre de serveurs Web configurables varie selon les modèles de boîtiers :

Modèle	Nbre max. serveurs HTTP	Nbre max. serveurs Autres
U30, U70	64	32
U120, U250, U450	128	64
U1100, U1500, NG1000-A	256	128
U6000, NG5000-A	512	256

Ajout d'un serveur web

Pour ajouter un serveur d'accès Web, suivez la procédure suivante :

1. Cliquez sur le bouton **Ajouter** puis sélectionnez l'un des serveurs proposés. Un écran contenant des noms de serveurs s'affiche.
2. Indiquez un nom pour ce serveur. (Le nom ne peut être vide, et les caractères autorisés sont : les chiffres, les lettres, l'espace, -, _, et le point.)
3. La configuration de ce serveur apparaît alors, les explications des différents paramètres sont données ci-dessous.

Serveur de destination	Le champ permet de spécifier l'objet correspondant au serveur auquel l'utilisateur pourra accéder. **AVERTISSEMENT** Veillez à utiliser un objet dont le nom est identique au nom **FQDN** du serveur auquel il fait référence. Si cela n'est pas le cas (nom de l'objet : webmail, nom FQDN : www.webmail.com par exemple), il est possible que les requêtes du firewall auprès de ce serveur soient refusées.
Port	Champ permettant de spécifier le port du serveur auquel l'utilisateur veut accéder. Le port défini est 80 pour http.
URL : chemin d'accès	Cette URL permet d'arriver directement sur la page spécifiée.
URL utilisée par le VPN SSL	Lien calculé selon les 3 champs **Serveur de destination**, **Port** et **URL : chemin d'accès**. (Exemple : http://serveur de destination/URL : chemin d'accès).
Nom du lien sur le portail utilisateur	Le lien défini apparaît sur le portail Web NETASQ. Lorsque l'utilisateur clique sur ce lien, il est redirigé vers le serveur correspondant.

Configuration avancée

Activer la liste blanche d'URLs	Seuls les liens réécrits par le module VPN SSL sont accessibles au travers du VPN SSL. S'il existe sur un site autorisé un lien vers un site Web extérieur (dont le serveur n'est pas défini dans la configuration VPN SSL), celui-ci sera inaccessible par le VPN SSL. Lorsque la liste blanche est activée, elle permet l'accès à des URL qui ne seraient pas réécrites via le champ **Ne pas réécrire les URLs du groupe.**

	Par exemple, pour un accès vpnssl webmail, si l'on souhaite autoriser les utilisateurs à quitter le vpnssl en cliquant sur les liens contenus dans leurs mails, dans ce cas il faut ajouter une liste blanche contenant « * ».  **AVERTISSEMENT** Lorsqu'un lien de cette liste blanche est cliqué par un utilisateur, celui-ci n'est plus protégé par le module de VPN SSL NETASQ.
Ne jamais afficher ce serveur sur le portail utilisateur (accès via un autre serveur uniquement)	Tous les serveurs configurés dans la configuration du VPN SSL sont par défaut indiqués sur le portail d'authentification NETASQ. Toutefois il pourrait être nécessaire qu'un de ces serveurs ne soit accessible que par l'intermédiaire d'un autre serveur, alors, dans ce cas, il faudrait cocher l'option « Ne pas afficher ce serveur sur le portail ». En effet lorsque cette option est cochée dans la configuration d'un serveur, ce serveur est accessible par le VPN SSL mais n'est pas présent dans la liste d'accès direct. Il faut un lien sur un serveur vers ce serveur pour y accéder. Une application peut utiliser plusieurs serveurs mais n'avoir qu'un seul point d'entrée, donc un seul lien dans le menu du portail.
Désactiver la méthode d'authentification NTLM	Certains serveurs Web peuvent demander une authentification préalable au transfert de flux entre le serveur et l'utilisateur. Ne supportant pas cette méthode d'authentification pour les trafics traversant le firewall, celle-ci peut être désactivée.
Réécrire le champ « User-Agent » (force le mode compatibilité d'OWA)	Le champ "User-Agent" de l'entête d'une requête HTTP contient l'identifiant de navigateur Web utilisé par l'utilisateur. Pour Internet Explorer par exemple : Mozilla/4.0 (compatible; MSIE 6.0 ...). La réécriture du "User-Agent" permet donc de modifier la requête HTTP de telle façon que l'on pense qu'elle provient d'un autre type de navigateur qu'en réalité. Cette option est notamment utile dans une utilisation dégradée d'Outlook **Web Access** (OWA). En effet, **Outlook Web Access** (OWA) en mode premium, mode très évolué d'Outlook **Web Access** fait appel au Webdav, une extension du protocole HTTP. Ces extensions n'étant pas supportées par tous les équipements réseau (le mode premium d'OWA est supporté par le module VPN SSL des firewalls NETASQ), le transit de ces trafics pourrait poser des problèmes de compatibilité en particulier sur Internet. Plutôt que de devoir dégrader l'utilisation d'OWA pour tous les utilisateurs (interne et externe), l'option **Réécriture du User-Agent** permet une utilisation "premium" de OWA en interne (compatibilité avec le mode premium facile à obtenir) et une utilisation "dégradée" en passant par le VPN SSL (utilisé par les utilisateurs nomades, via Internet). En effet les "vieux" navigateurs Web ne supportent pas ces extensions, OWA fonctionne donc automatiquement en mode dégradé lorsqu'il rencontre le "User-Agent" de ces navigateurs.
Réécrire le code spécifique au mode Premium d'OWA	En cochant cette option, vous activez les règles spécifiques de réécriture permettant de supporter Outlook Web Access en mode premium.
Réécrire le code spécifique à Lotus Domino	En cochant cette option, vous activez les règles spécifiques de réécriture permettant de supporter les applications Web de Lotus domino.

URLs alternatives pour ce serveur (alias)

Alias du serveur	Les alias permettent d'indiquer au module VPN SSL que le serveur possède plusieurs noms et/ou adresses IP. Si un serveur de mails est défini comme l'objet « webmail.intranet.com » auquel on assigne l'alias "192.168.1.1", lorsque le lien visité sera « http://webmail.intranet.com » ou "http://192.168.1.1" l'utilisateur sera redirigé vers le serveur de mails. En cliquant sur le bouton **Ajouter**, une ligne s'affiche vous permettant d'ajouter un nouvel alias.

Ajout d'un serveur web OWA

Le module **VPN SSL** des firewalls NETASQ supporte les serveurs OWA ("Outlook Web Access") : Exchange 2003, 2007, 2010.

Le mode « Premium » est utilisable sous Windows avec Internet Explorer 5 ou + uniquement. Il est basé sur les technologies web comme html, css, javascript mais également sur des technologies propriétaires Microsoft comme htc, xml, activeX.
En Exchange 2003, les liens sont des liens absolus que ce soit dans les pages HTML, les scripts javascripts, dans les données XML, dans les feuilles XSL. C'est-à-dire de type http://www.netasq.com/index.htm.

Il est donc possible d'ajouter dans la liste des serveurs d'accès Web, un serveur HTTP avec certaines options spécifiquement pré remplies pour une parfaite compatibilité avec OWA.

Pour ajouter un serveur HTTP-OWA, suivez la procédure suivante :

1. Cliquez sur le bouton **Ajouter** puis sélectionnez `Serveur web OWA 2003 (mode Premium)` ou `Serveur web OWA 2007 – 2010 (mode premium)`. L'écran suivant s'affiche :
2. Indiquez un nom pour ce serveur. (Le nom ne peut être vide, et les caractères autorisés sont : les chiffres, les lettres, l'espace, -, _, et le point.)
3. Les options pré-remplies pour un serveur OWA 2003 premium sont : le port « http », le champ **URL : chemin d'accès** avec l'indication "exchange", LE CHAMP **Activer la liste blanche d'URLs** coché, le champ **Ne pas réécrire les URLs du groupe** avec l'indication « vpnssl_owa », le champ **Désactiver la méthode d'authentification NTLM** et le champ **Réécrire le code spécifique au mode Premium d'OWA**.

Pour un serveur OWA 2007-2010, les champs préremplis sont : le port http, le champ **URL : chemin d'accès** avec l'indication "owa", le champ **Activer la liste blanche d'URLs** avec l'indication du groupe d'URL « vpnssl_owa », et le champ **Réécrire le code spécifique au mode Premium d'OWA**.
Les autres options non remplies doivent être configurées de la même manière que pour un serveur d'accès Web "normal".

Ajout d'un serveur web Lotus Domino

Le module **VPN SSL** des firewalls NETASQ supporte les serveurs Lotus domino.
Il est possible d'ajouter dans la liste des serveurs d'accès Web, un serveur HTTP avec certaines options spécifiquement pré remplies pour une parfaite compatibilité avec LOTUS DOMINO.

Pour ajouter un serveur HTTP-Lotus domino, suivez la procédure suivante :

1. Cliquez sur le bouton **Ajouter** puis sélectionnez **Serveur web Lotus Domino**.
2. Indiquez un nom pour ce serveur. (Le nom ne peut être vide, et les caractères autorisés sont : les chiffres, les lettres, l'espace, -, _, et le point.)
3. Les options pré-remplies pour un serveur Lotus domino sont les champs : Port « http » et **Réécrire le code spécifique à Lotus Domino**.

L'onglet « Serveurs applicatifs »

Configuration avec un serveur applicatif

Pour ajouter un serveur d'accès aux ressources autres que le type Web, suivez la procédure suivante :

1. Cliquez sur le bouton **Ajouter** puis sélectionnez **`Serveur applicatif.`**
2. Indiquez un nom pour ce serveur. (Le nom ne peut être vide, et les caractères autorisés sont : les chiffres, les lettres, l'espace, -, _, et le point.)
3. La configuration de ce serveur apparaît alors, les explications des différents paramètres sont données ci-dessous.

Serveur de destination	Ce champ permet de spécifier l'objet correspondant au serveur auquel l'utilisateur pourra accéder.
Port	Ce champ permet de spécifier le port sur le serveur auquel l'utilisateur pourra accéder.

Paramètres du poste utilisateur

Adresse IP d'écoute (locale)	Choix de l'adresse locale du client.
Port	Ce port situé sur la station distante est utilisé par l'applet JAVA pour la redirection des flux chiffrés à destination du firewall NETASQ. Notez que l'utilisateur doit posséder certains droits sur ce port (pour l'ouverture par exemple), veillez donc à modifier les droits locaux d'administration de la machine en conséquence. De plus, le port spécifié doit être libre d'utilisation sur toutes les machines désirant se connecter au serveur associé via le portail.

Configuration avancée

Activer la compatibilité Citrix	Permet d'activer la compatibilité avec le portail Web d'authentification et l'accès via navigateur Web. Cette option est inutile si le client lourd Citrix est utilisé.
Commande exécutée au démarrage	Exécutée au lancement de l'applet, cette commande permet à l'administrateur de définir des actions préalables à l'affichage du serveur. Par exemple, cette commande pourrait lancer un script présent sur un serveur et qui vérifierait l'activité de l'antivirus présent sur la machine de l'utilisateur avant de lui donner accès au serveur.

Configuration avec un serveur Citrix

1. **Etape 1 : Création d'un objet pour le serveur Citrix**
   Accédez à la base d'objets afin de créer une machine puis sélectionnez une machine.
2. **Etape 2 : Configuration d'un serveur applicatif**
   Depuis le module `VPN SSL`, sélectionnez l'onglet `Serveurs applicatifs`. Cliquez sur le bouton Ajouter puis sélectionnez `Serveur Citrix`. Donnez un nom à votre serveur. L'écran de configuration du serveur Citrix s'affiche.
   Sélectionnez le serveur Citrix créé précédemment dans la base d'objets *(Cf. Etape1)*

Etape 3 : Configuration d'un Serveur web

Sélectionnez l'onglet `Serveurs web`.
Cliquez sur le bouton Ajouter puis sélectionnez "Serveur web". Donnez un nom à votre serveur.
L'écran de configuration du serveur Web s'affiche.
Au niveau de l'URL : chemin d'accès, indiquez CitrixAccess/auth/login.aspx (s'il s'agit de la version Presentation Server 4.0).

Envoi de la configuration

Cliquez sur le bouton Appliquer.

Accès au portail Web

Ouvrez un navigateur Web puis identifiez –vous (https://adresse IP de votre firewall ou son nom).

Allez dans "Accès sécurisé" puis sélectionnez dans la liste déroulante "Ouvrir l'accès sécurisé dans un pop-up".

AVERTISSEMENT

Il est important que l'applet VPN SSL NETASQ fonctionne en tâche de fond.
Sélectionnez ensuite **`Accès portail\Portail`** puis saisissez votre nom d'utilisateur, votre mot de passe et le domaine.

Suppression d'un serveur

Pour supprimer un serveur, suivez la procédure suivante :

1. Sélectionnez le serveur à supprimer.
2. Cliquez sur le bouton **Supprimer**.

AVERTISSEMENT

Lorsqu'un serveur est retiré de la liste des serveurs VPN SSL configurés, il est automatiquement retiré des profils desquels il faisait partie.

L'onglet « Profils utilisateurs »

Principe de fonctionnement

Par défaut tous les serveurs configurés dans le module `VPN SSL` sont affichés sur le portail d'authentification. Ainsi tous les utilisateurs ayant droit aux fonctionnalités de VPN SSL offertes au firewall ont accès à tous les serveurs configurés par l'administrateur. La notion de profil permet de déterminer quels utilisateurs auront accès à quels serveurs configurés dans le VPN SSL.

Configuration d'un profil

Ajout d'un profil

Pour ajouter un profil dans la liste des profils VPN SSL disponibles, référez-vous à la procédure suivante :

1. Cliquez sur le bouton **Ajouter** puis spécifiez le nom du profil.
2. Sélectionnez dans les listes : « Serveurs web accessibles » et « Serveurs applicatifs accessibles » les serveurs qui seront accessibles aux utilisateurs appartenant à ce profil.
3. Cliquez sur **Appliquer** pour activer la configuration.

> **AVERTISSEMENT**
> Il est impossible de créer un profil s'il n'existe pas au minimum un serveur VPN SSL configuré.

Suppression d'un profil

Pour supprimer un profil, référez-vous à la procédure suivante :

1. Sélectionnez le profil à supprimer.
2. Cliquez sur le bouton **Supprimer**.

Utiliser un profil

Un profil peut être utilisé de 2 manières différentes. Soit il est utilisé comme profil par défaut dans la configuration du VPN SSL, soit il est assigné à un ou plusieurs utilisateurs comme profil spécifique de ces utilisateurs.

<u>Utiliser un profil comme profil par défaut</u>

Pour utiliser un profil comme profil par défaut de la configuration VPN SSL (tous les utilisateurs n'utilisant pas de profil spécifique seront affectés par ce profil par défaut), référez-vous à la procédure suivante :

1. Créez un profil dans VPN SSL\Profils utilisateurs,
2. Définissez le profil qui sera utilisé comme profil par défaut (nom du profil et serveurs associés) dans le menu de configuration Utilisateurs\Droits d'accès\Options par défaut\VPN SSL.

<u>Utiliser un profil comme profil spécifique d'un ou plusieurs utilisateurs.</u>

Pour utiliser un profil comme profil spécifique d'un ou plusieurs utilisateurs (quelle que soit la liste des serveurs définis par le profil par défaut, ces utilisateurs posséderont une liste de serveurs spécifiques), référez-vous à la procédure suivante :

1. Définissez le profil qui sera utilisé comme profil spécifique (nom du profil et serveurs associés) dans `Profils utilisateurs` du module `VPN SSL` puis appliquez les modifications en cliquant sur **Appliquer.**
2. Dans le module `Utilisateurs\Droits d'accès\Configuration par l'utilisateur`, choisissez l'utilisateur puis dans la colonne « VPN SSL », choisir le profil défini au préalable et cliquez sur le bouton **Appliquer**.

Services VPN SSL sur le portail Web NETASQ

Lorsque l’authentification sur le firewall est activée (module `Utilisateurs\ Authentification\` onglet `Général`, et coche « Activer le portail captif »), vous pouvez accéder aux fonctionnalités du VPN SSL NETASQ.

Pour accéder aux fonctionnalités du **VPN SSL**, suivez la procédure suivante :

1. Ouvrir un navigateur Web.
2. Indiquer dans la barre d’adresse, l’URL : https://Adresse_Firewall.
3. La page d’authentification sur le firewall apparaît, vous devez vous connecter.
4. Si vous possédez des droits sur l’utilisation des fonctionnalités VPN le menu **`Accès sécurisé`** apparaît. Il permet d’accéder aux fonctionnalités VPN SSL.

A partir de la version 9.0.1, lorsque la durée d’authentification est expirée ou que l’accès au VPN SSL est refusé, l’utilisateur sera redirigé vers la page d’authentification transparente (SSO) si cette méthode est disponible.

Accédez aux sites Web de votre entreprise par un tunnel SSL

Ce menu présente les sites Web configurés par l’administrateur et auxquels les utilisateurs peuvent accéder.
Les autres accès sécurisés permettent d’accéder au menu des autres sites sécurisés configurés par l’administrateur.

Accédez aux ressources de votre entreprise par un tunnel SSL

Ce menu présente les autres serveurs configurés par l’administrateur et auxquels les utilisateurs peuvent accéder.



Sur cette page aucun lien n’est disponible. Il est pourtant indispensable que cette fenêtre reste ouverte pendant toute la durée de la connexion (elle peut être minimisée). La fermeture de la fenêtre entraîne la coupure de la connexion.

Pour accéder aux ressources configurées par l’administrateur, il s’agit d’indiquer au logiciel client, un client de messagerie par exemple, que le serveur auquel il doit se connecter pour récupérer les mails n’est plus le serveur mail habituel mais il faut lui indiquer une adresse du type "127.0.0.1:Port_Ecoute" où "Port_Ecoute" est le port spécifié dans la configuration du serveur.
Le port d’écoute pour chacun des serveurs configurés est rappelé dans la page du portail Web NETASQ.



documentation@netasq.com